Pinja Turunen

Todentamisen ohittaminen: tutkimuksen nykytilanne

Tietotekniikan pro gradu -tutkielma

29. toukokuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Pinja Turunen

Yhteystiedot: pinja.k.turunen@gmail.com

Ohjaaja: Timo Hämäläinen

Työn nimi: Todentamisen ohittaminen: tutkimuksen nykytilanne

Title in English: Authentication Bypass: The Current Status of Research

Työ: Pro gradu -tutkielma

Opintosuunta: Ohjelmisto- ja tietoliikennetekniikka

Sivumäärä: 50+25

Tiivistelmä: Tässä tutkimuksessa tehtiin systemaattinen kirjallisuuskartoitus selvittämään todentamisen ohittamiseen liittyvän tutkimuksen nykytilannetta, vertaillen julkaisuja ja samalla aikavälillä havaittuja haavoittuvuuksia. Tutkitut julkaisut kuvasivat pääasiassa ratkaisuja todentamisen ohittamisen estämiseksi, mutta myös hyökkäyksiä läpikäyviä julkaisuja oli paljon. Tutkimuksessa yleisimpiä käsiteltyjä aihealueita olivat laitteisiin ja yhteyksiin liittyvä todentamisen ohittaminen sekä biometrisen todentamisen haavoittuvuudet. Aiheeseen liittyvissä väärän todennuksen (CWE-287) alakategorioissa julkaisuista ja haavoittuvuuksista yleisin oli todentamisen ohittaminen huijaamisen kautta. Toisena julkaisuista oli toiston kautta todentamisen ohittaminen. Haavoittuvuuksissa toisiksi yleisimpänä oleva vaihtoehtoisen reitin tai kanavan käyttäminen sen sijaan esiintyi vähemmän julkaisuissa, mahdollisesti kaivaten lisätutkimusta.

Avainsanat: todentaminen, ohittaminen, haavoittuvuus, hyökkäys, kirjallisuuskartoitus

Abstract: A systematic mapping study was conducted to assess the current status of research on authentication bypass, comparing studies and vulnerabilities occurring around the same time. Found studies mostly described solutions to prevent authentication bypass, but many also described attacks. In the research, the most common topics were authentication bypass in devices and connections, and vulnerabilities of biometric authentication. In the subcategories of improper authentication (CWE-287) relating to authentication bypass, the

most common one in studies and vulnerabilities was authentication bypass by spoofing. The second in studies was bypass by capture-replay. In vulnerabilities, the second most common was bypass by alternate path or channel, which appeared less in studies, possibly needing further research.

Keywords: authentication, bypass, vulnerability, attack, systematic mapping

Kuviot

Taulukot

Sisällys

1 Johdanto

Nykyään ihmisillä on lukuisia käyttäjiä erilaisissa palveluissa, joissa heidän tulee todentaa itsensä kirjautuakseen sisään järjestelmiin. Näiden todennusten takana voi olla tallessa henkilökohtaista tietoa, kuten kotiosoite tai henkilötunnus, tai esimerkiksi yrityssalaisuuksia. Näiden tietojen paljastumista ulkopuolisille voidaan pitää vakavana tietoturvan ongelmana.

Jokaisella meistä on lukuisia salasanoja muistettavana. Uusia salasanoja luotaessa on entistäkin enemmän vaatimuksia niiden suhteen: niistä pitäisi tehdä tarpeeksi pitkiä ja monimutkaisia, ettei niitä arvattaisi helposti, mutta toisaalta niiden määrän jatkuvasti kasvaessa näiden vaikeiden salasanojen muistaminen voi olla entistäkin hankalampaa. Siitäkin huolimatta, vaikka onnistuisi luomaan ja pitämään tallessa näitä lukuisia monimutkaisia salasanoja, esimerkiksi hyödyntämällä salasanageneraattoria ja -hallintaohjelmaa, tämä haaste ei itsessään ratkaise kaikkia kirjautumiseen liittyviä tietoturvan ongelmia.

Todentamisen ohittaminen on hyökkäys, jossa hyökkääjä ohittaa nämä kirjautumiset eri tavoin. Tällaisissa hyökkäyksissä loppukäyttäjien salasanojen monimutkaisuus ei riitä, vaan järjestelmän kehittäjät ja ylläpitäjät ovat vastuussa todentamisen oikeaoppisesta toiminnasta. Todentamisen ohittamisen hyökkäykset ovat mahdollisia erilaisten järjestelmässä olevien haavoittuvuuksien avulla – oli ne sitten kovakoodattuja ylläpitäjän tunnuksia tai syvällä kirjastojen uumenissa piileviä suunnitteluvirheitä.

Tutkimukseni tarkoituksena on tarkastella todentamisen ohittamiskeinoihin liittyvän tutkimuksen nykytilannetta – miten ja millaisia erilaisia todentamisen ohittamiskeinoja on tutkittu. Tutkimuksen tilaa verrataan samalla ajanjaksolla löytyneisiin todentamisen ohittamisen haavoittuvuuksiin. Tutkimalla aiheen nykytilannetta voidaan esimerkiksi nähdä mitkä todentamisen ohittamisen keinot ovat tällä hetkellä kiinnostuksen kohteina aiheen tutkimuksessa verrattuna haavoittuvuuksiin.

2 Todentaminen

Käyttäessämme kirjautumista vaativia palveluita, käytämme tunnistusta (engl. *identification*), **todentamista** (engl. *authentication*) sekä valtuutusta (engl. *authorization*) (Zviran ja Erlich 2006, s. 91). Tunnistuksella tarkoitetaan sitä, kun käyttäjä kertoo järjestelmälle kuka hän on – esimerkiksi käyttäjä- tai henkilötunnuksen kautta – jonka jälkeen todentamisen kautta varmistetaan, onko käyttäjä kuka hän väittää olevansa (Grassi, Fenton ja Garcia 2017, s. 41; Stouffer ym. 2015, s. B-7; Grance ym. 2002, s. D-1). Todentamisen erilaiset tavat perustuvat **todentamistekijöihin** – todisteeksi tarvitaan joko jotain mitä käyttäjä tietää (engl. *something you know*), mitä hän omistaa (engl. *something you have*) tai mitä hän on (engl. *something you are*) (Grassi ym. 2017, s. 13–26). Suomen laissa (8 a § (29.6.2016/533)) näistä todentamistekijöistä käytetään, samassa järjestyksessä, termejä tiedossa oloon perustuva, hallussapitoon perustuva sekä luontainen todentamistekijä (Finlex 2009). Jos käyttäjä todennetaan onnistuneesti, tämän jälkeen voidaan suorittaa valtuutuksia, joiden kautta selvitetään, onko käyttäjällä oikeuksia tiettyihin resursseihin järjestelmässä (Stouffer ym. 2015, s. B-2; Shirey 2007).

Todentamistapoja on käytössä useita erilaisia. Grassi ja hänen kollegansa (2017, s. 13–23) mainitsevat tällaisiksi muutaman erilaisen vaihtoehdon. Yleisimmin käytössä nähdään muistetut salaisuudet, jotka perustuvat tiedossa oloon. Näitä ovat tyypillisesti salasanat tai PIN-koodit. Näiden lisäksi on hallussapitoon perustuvia etsittäviä salaisuuksia, joina käytetään esimerkiksi tunnuslukukorttia tai vastaavaa digitaalista versiota tarjoamaan käytettävä salasana. On myös olemassa kertakäyttöisen kirjautumiskoodin (engl. *one-time password*, OTP) tarjoavia laitteita tai ohjelmia, sekä kryptografisia laitteita tai ohjelmia.

Erityisesti viime vuosina luontaisiin todentamistekijöihin perustuva biometrinen todentaminen on kasvattanut suosiotaan. Biometrisia todentamisen tapoja, kuten sormenjälkeä, käytetään usein erityisesti mobiililaitteissa. Rui ja Yan (2019, s. 7) nostavat esiin biometristä todentamista käsittelevässä tutkimuksessaan sormenjäljen lisäksi käden, kasvojen, iiriksen, äänen, näppäilyn, kosketuksen sekä sydänsähkökäyrän avulla tehtävän todentamisen. Ometovin ja muiden (2018, s. 19) mukaan käyttäjä voidaan todentaa myös esimerkiksi käytöksen perusteella, kuten kirjoituksen tai liikehdinnän kautta.

Näitä erilaisiin todentamistekijöihin perustuvia todentamistapoja voidaan myös hyödyntää yhdessä, näin käyttäen monivaiheista todentamista (engl. *multi-factor authentication*, MFA) todentamisen vahvistamiseksi (Grassi ym. 2017, s. 12). Lisäksi sekä kryptografisissa että OTP:ita tarjoavissa ohjelmissa ja laitteissa voidaan itsessään hyödyntää monivaiheisuutta, vaatien esimerkiksi biometristä tai salasanan kanssa todentamista ennen salatun tiedon paljastamista alkuperäistä todentamista varten (Grassi ym. 2017, s. 20,23–24).

Kirjautumisessa on myös mahdollista käyttää monivaiheista todentamista ainoastaan silloin, jos todentamisessa havaitaan jotain poikkeavaa. Riskipohjaisessa todentamisessa (engl. *risk-based authentication*, RBA) hyödynnetään todentamisen kontekstia määrittämään tarvitaanko todentamisessa lisävaiheita (Wiefling, Lo Iacono ja Dürmuth 2019, s. 2). Wiefling, Lo Iacono ja Dürmuth (2019, s. 11) löysivät tutkimuksessaan, että esimerkiksi IP-osoitteen, käytettävän ohjelman sekä näytön resoluution eroja kirjautumiskertojen välillä voidaan hyödyntää määrittämään riskiä ja näin tarvetta lisätodentamiselle. Todentaminen on tällöin nopeampaa kontekstillisten piirteiden pysyessä samana, mutta samalla monivaiheisen todentamisen hyödyt tulevat esiin kontekstin muuttuessa.

Järjestelmissä kirjautuminen tyypillisesti suoritetaan ensin niin sanotussa sisääntulopisteessä (engl. *entry-point authentication*), jonka jälkeen käyttäjän oletetaan pysyvän samana. Tästä oletuksesta poikkeavat järjestelmät, joissa käytetään jatkuvaa todentamista (engl. *continuous authentication*). Jatkuvassa todentamisessa todentamista ylläpidetään esimerkiksi tarkkailemalla näytön kosketuksia käyttäjän navigoidessa mobiililaitteellaan (Frank ym. 2012, s. 1–2). Jatkuvaa todentamista voidaan käyttää yksinään tai yhdessä sisääntulopisteessä tehtävän todentamisen kanssa (Frank ym. 2012, s. 1).

Todentamiseen liittyen on kuitenkin hyvä huomata, ettei todentamisessa ole aina ihmistä käyttäjänä, vaan todentamista tapahtuu myös laitteiden välisessä kommunikoinnissa. Esimerkiksi lähivuosina pinnalle noussut esineiden internet (engl. *Internet of Things*, IoT) käyttää laitteiden välistä kommunikointia ja voi näin hyödyntää todentamista laitteiden välillä (Ren ym. 2013, s. 1). Laitteiden välisessä todentamisessa ei kuitenkaan voida käyttää kaikkia samoja todentamistapoja kuin käyttäjän ollessa ihminen (Ren ym. 2013, s. 1). Ren ja hänen kollegansa (2013, s. 8) kuvaavat laitteiden välisen todentamisen malleiksi tunnus-, metriikka-, referenssi- ja todistajapohjaiset todentamisen mallit. Kuitenkin osa laitteiden vä-

lisistä todentamisen tavoista on lähellä ihmisten käyttämää todentamista, esimerkiksi metriikkapohjainen todentaminen on hyvin lähellä biometrista todentamista (2013, s. 6). Se voi perustua esimerkiksi laitteesta syntyvään ”sormenjälkeen”, joka pohjautuu laitteen uniikkiin ominaisuuteen (Lalouani ym. 2020, s. 1).

3 Todentamisen ohittaminen

Todentamisen ohittaminen (engl. *authentication bypass*) on todentamismekanismin haavoittuvuuteen kohdistettu hyökkäystapa, jossa hyökkääjä ohittaa tai väärennetysti läpäisee todentamisen (MITRE 2021a). Hyökkäys voi estää tietojärjestelmän luottamuksellisuuden, eheyden ja saavutettavuuden, eli niin sanotun CIA-kolmion (engl. ***C****onfidentiality*, ***I****ntegrity* ja ***A****vailability*) (Cawthra ym. 2020, s. 8; Barker ym. 2010, s. 41), sekä oikeuksien valvonnan toteutumisen (MITRE 2021g, s. 642).

Todentamisen ohittamisen hyökkäyksen avulla hyökkääjä voi saada oikeuksia järjestelmässä, jotka eivät kuulu hänelle (MITRE 2021a). Näihin lukeutuvat esimerkiksi käyttäjän esittäminen ja hänen tietojensa lukeminen sekä koodin tai komentojen ajaminen (MITRE 2021g, s. 642). Oikeuksien laajuus on riippuvaista käyttäjästä, jonka oikeudet hyökkääjä saavuttaa hyökkäyksen avulla. Esimerkiksi yksittäisen peruskäyttäjän kohdalla voi päästä käsiin vain hänelle näkyvissä oleviin tietoihin, kun taas ylläpitäjän käyttäjällä voi olla järjestelmän hallintaan liittyviä oikeuksia.

3.1 Haavoittuvuudet

Todentamisen ohittamisen mahdollistavia haavoittuvuuksia, joista käytetään myös nimeä takaovi (engl. *backdoor*) (Shoshitaishvili ym. 2015, s. 1), on monia erilaisia. Todentamisen ohittamisen mahdollistaviin haavoittuvuuksiin kuuluu niin vahingossa kuin tarkoituksellisesti laitettuja haavoittuvuuksia (Shoshitaishvili ym. 2015, s. 1–2). Tarkoituksellisista haavoittuvuuksista osa on kehittäjien laittamia, osa hyökkääjien (Wilhelm ja Andress 2011, s. 269).

3.1.1 Tarkoituksellisesti jätetyt takaovet

Vaikka toivoisi todentamisen ohittamisen haavoittuvuuksien olevan syntyneen vahingossa eikä ilkimielisessä tarkoituksessa, osa näistä haavoittuvuuksista on myös tarkoituksellisesti jätettyjä haavoittuvuuksia. Esimerkiksi järjestelmiin kovakoodattuja ylläpitäjien tunnuksia havaitaan jatkuvasti lisää, vaikka tämä on hyvin tunnettu haavoittuvuuden tyyppi. Osaa näistä tapauksista voidaan pitää vahinkoina, esimerkiksi jäänteinä järjestelmän kehitysprosessista,

mutta se ei vaikuta selittävän kaikkia tapauksia miksi järjestelmiin jäisi helposti vältettäviä haavoittuvuuksia.

Tarkoituksellisesti jätettyjä takaovia voidaan käyttää esimerkiksi teknisen tuen työkaluina järjestelmien ylläpitoon liittyen (Shoshitaishvili ym. 2015, s. 1–2), jota voidaan kuitenkin pitää vähintäänkin kyseenalaisena ratkaisuna. Osa takaovista on myös puhtaasti ilkimielisiä hyökkääjien jättämiä haavoittuvuuksia (Wilhelm ja Andress 2011, s. 269). Kuitenkin tarkoituksesta riippumatta tarkoituksellisesti jätetyt takaovet vaarantavat järjestelmän turvallisuutta, sillä ne tarjoavat helpomman reitin päästä käsiksi järjestelmään hyökkäystarkoituksessa (Shoshitaishvili ym. 2015, s. 3).

3.1.2 Väärän todentamisen haavoittuvuudet

Todentamisen ohittamisen mahdollistavia haavoittuvuusluokituksia (*Common Weakness Enumeration*, CWE) on useita, ja niitä on luokiteltu luokan CWE-287 *Improper Authentication* eli väärän todennuksen alle (MITRE 2021g, s. 640). Väärä todennus löytyy vuoden 2021 OWASP Top 10 -listalta kategorian A07 *Identification and Authentication Failures* eli tunnistamisen ja todentamisen vikojen alta (OWASP 2021a). Vaarallisimpia haavoittuvuusluokituksia muokatulla kaavallaan etsineet Galhardo ja hänen kollegansa (2020, s. 163–164) nostivat myös väärän todentamisen korkealle sijalle listallaan.

MITRE (2021g, s. 640–641) luokittelee väärän todennuksen alle 27 alaluokitusta. Jos käyttäjän annetaan luoda liian heikko salasana (CWE-521: *Weak Password Requirements*) tai todentamiseen ei vaadita useampaa erilaista keinoa (CWE-308: *Use of Single-factor Authentication*), erityisesti pelkän salasanan lisäksi (CWE-309: *Use of Password System for Primary Authentication*), voidaan todentamisessa nähdä olevan haavoittuvainen (MITRE 2021g, s. 693–697, 1113–1115). Lukuisten peräkkäisten kirjautumisyritysten seurauksena tulisi toteuttaa väliaikainen esto (CWE-307: *Improper Restriction of Excessive Authentication Attempts*), mutta siitä ei kuitenkaan saa tehdä liian estävää, haitaten todellista käyttäjää (CWE-645: *Overly Restrictive Account Lockout Mechanism*) (MITRE 2021g, s. 688–692, 1294–1295). Kirjautumiseen voi olla liitettynä CAPTCHA-testi yrittämään estää esimerkiksi liikaa salasanan yrittämistä ohjelmallisesti, mutta myös CAPTCHA voi olla liian helppo, jotta siitä

olisi tarpeeksi hyötyä (CWE-804: *Guessable CAPTCHA*) (MITRE 2021g, s. 1532–1533).

Salasanan vaihtamisprosessiin, jonne mennään esimerkiksi salasanan unohtaessa, on myös mahdollista syntyä tietoturvan kannalta vakavia haavoittuvuuksia, jos siinä ei vaadita sopivaa todentamista (CWE-620: *Unverified Password Change*, CWE-640: *Weak Password Recovery Mechanism for Forgotten Password*) (MITRE 2021g, s. 1256–1258, 1280–1282). Myöskin salasanan säilyttäminen liian kevyin suojauksin on ongelmallista salasanojen salassapysymisen kannalta (CWE-261: *Weak Encoding for Password*, CWE-522: *Insufficiently Protected Credentials*) (MITRE 2021g, s. 584–586, 1116–1119). Salasanoja ei tulisi laittaa kovakoodattuina esimerkiksi koodi- tai asetustiedostoihin (CWE-798: *Use of Hard-coded Credentials*) (MITRE 2021g, s. 1522–1530) – tällaiset löytyvät ”anteeksiantamattomien haavoittuvuuksien” listalta, johon on kirjattu tunnettuja yksinkertaisesti hyökättäviä haavoittuvuuksia (Christey 2007, s. 5). Salasanalle voidaan määrittää vanhenemisaika, jonka jälkeen käyttäjän tulee luoda uusi salasana: jos tällaista ei toteuteta (CWE-262: *Not Using Password Aging*), tai määritetty aika on liian pitkä tehden sen irrelevantiksi (CWE-263: *Password Aging with Long Expiration*), voidaan myös tämä nähdä todennuksen kannalta ongelmallisena (MITRE 2021g, s. 585–589).

Palveluihin, joissa on asiakasohjelman lisäksi palvelin, tulee toteutuksessa kiinnittää huomiota, ettei todentamista tai sen osia suoriteta virheellisesti käyttäjän puolella palvelimen sijaan (CWE-603: *Use of Client-Side Authentication*, CWE-836: *Use of Password Hash Instead of Password for Authentication*) (MITRE 2021g, s. 1231–1232, 1587–1588), esimerkiksi mahdollistamalla todentamisen ohittamisen yksinkertaisesti laittamalla evästeeseen `authenticated=1` (Christey 2007, s. 5). Huomiota tulee myös kiinnittää sertifikaattien oikeaoppiseen käyttöön (CWE-295: *Improper Certificate Validation*) ja että todentaminen toteutetaan kaikissa kriittisissä funktioissa (CWE-306: *Missing Authentication for Critical Function*) (MITRE 2021g, s. 658–662, 684–688).

Todentamisalgoritmiin tai -protokollaan voi liittyä erilaisia haavoittuvuuksia. Esimerkiksi on mahdollista, että ne ovat puutteellisesti toteutettuja (CWE-304: *Missing Critical Step in Authentication*), mahdollistavat reflektiohyökkäyksen (CWE-301: *Reflection Attack in an Authentication Protocol*) tai todentamisprosessi antaa käyttää todentamisalgoritmista virheellistä toteutusta (CWE-303: *Incorrect Implementation of Authentication Algorithm*) (MITRE

2021g, s. 676–678, 680–683).

Väärän todennuksen alta löytyy useampia nimensä mukaisesti todentamisen ohittamiseen liittyviä alaluokituksia. Näihin kuuluvat väärän tai vaihtoehtoisen reitin, kanavan (CWE-288: *Authentication Bypass Using an Alternate Path or Channel*) tai nimen käyttö (CWE-289: *Authentication Bypass by Alternate Name*) todentamisen ohittamiseksi (MITRE 2021g, s. 646–650). Vaihtoehtoinen reitti voi olla esimerkiksi se, jos ylläpitäjille tarkoitettu hallintasivu on jätetty vapaasti saavutettavaksi verkko-osoitteen avulla ilman tarkistuksia. Tällaisia haavoittuvuuksia voidaan myös pitää ”anteeksiantamattomana haavoittuvuutena” (Christey 2007, s. 5). Vaihtoehtoisella nimellä taas tarkoitetaan muun muassa syötteenvalidoinnin ongelmia, joissa koodattuja merkkejä ei käsitellä oikein (MITRE 2021g, s. 649). Esimerkiksi olisi ongelmallista, jos syöte hylätään sen sisältäessä `'` -merkin, mutta sen sijaan saman merkin prosenttikoodattu muoto `%27` hyväksyttäisiin.

Ohituksen voi suorittaa myös huijaamisen (CWE-290: *Authentication Bypass by Spoofing*) tai toiston (CWE-294: *Authentication Bypass by Capture-replay*) avulla (MITRE 2021g, s. 650–653, 657–658). Tässä tapauksessa huijaamisella tarkoitetaan sitä, että todentamiseen käytettävää dataa väärennetään niin, että sen avulla todentaminen voidaan ohittaa. MITRE (2021g, s. 651) antaa esimerkiksi tästä sen, että IP-osoite väärennetään todentamisen näkökulmasta luotettavaksi IP-osoitteeksi. Toistolla taas tarkoitetaan sitä, että todentaminen ohitetaan lähettämällä uudelleen kaapattuja todentamiseen liittyviä viestejä (MITRE 2021g, s. 657). Viestit voidaan lähettää joko alkuperäisessä muodossaan tai muokattuina (MITRE 2021g, s. 657).

Ohittamiseen voi myös liittyä väärä ymmärrys datan muuttumattomuudesta (CWE-302: *Authentication Bypass by Assumed-Immutable Data*, CWE-593: *Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created*) (MITRE 2021g, s. 679–680, 1208–1210). Todentaminen voi kuitenkin myös olla haavoittuvainen epäsuorasti toisen haavoittuvuuden kautta ja näin tulla ohitetuksi (CWE-305: *Authentication Bypass by Primary Weakness*) (MITRE 2021g, s. 683–684).

3.2 Hyökkäykset

Tunnettuja hyökkäystapoja luetteleva MITRE:n (2021a) CAPEC-luokittelu (engl. *Common Attack Pattern Enumeration and Classification*) sisältää todentamisen ohittamisen hyökkäystavan koodilla CAPEC-115. Siinä todentamisen ohittamisen alahyökkäystavoiksi luokitellaan pakotettu selaus, ohjelmointirajapinnan allekirjoituksen väärentäminen tiivistefunktion jatkeen haavoittuvuuden avulla, virtualisaation pakeneminen, palvelinpuolen pyynnönvääärennös sekä Bluetoothin avainneuvottelun hyökkäys.

MITRE (2021f) kuvaa pakotetun selauksen (CAPEC-87: *Forceful Browsing*) hyökkäystapana, jossa hyökkääjä menee hyökkäystarkoituksessa suoraan tiettyyn verkko-osoitteeseen. Hyökkääjä pyrkii pääsemään käsiksi sivuston osiin, joihin hänelle ei kuuluisi olla oikeuksia, kuten ylläpitäjien portaalisivulle. Tällainen hyökkäys on mahdollista, jos sivuja ei ole piilotettu tai niihin ei ole toteutettu asianmukaista kirjautumisen vaatimista niiden saavuttamiseksi. Hyökkäys kohdistuu väärän todentamisen haavoittuvuuksien alakategoriaan CWE-288 vaihtoehtoisen reitin tai kanavan käytöstä.

Toinen alahyökkäystapa on ohjelmointirajapinnan allekirjoituksen väärentäminen tiivistefunktion jatkeen haavoittuvuuden avulla (CAPEC-461: *Web Services API Signature Forgery Leveraging Hash Function Extension Weakness*) (MITRE 2021b). MITRE:n (2021b) mukaan tämän hyökkäyksen mahdollistaa tiettyjen tiivistefunktioiden, kuten SHA1 ja MD5, omaava haavoittuvuus liittyen niiden iteratiiviseen muotoon. Hyödyntäen tätä hajautusfunktion haavoittuvuutta hyökkääjä voi luoda aidon näköisen kutsun, johon hän voi samalla lisätä mukaan hyökkäysparametreja. Hyökkäys kohdistuu haavoittuvuuteen, jonka avulla hyökkääjä voi huijata järjestelmää pitämään häntä oikeana käyttäjänä, joka on väärän todentamisen haavoittuvuuksien alla oleva kategoria (CWE-290).

Virtualisaation pakeneminen (CAPEC-480: *Escaping Virtualization*) on hyökkäystapa, jossa MITRE:n (2021c) mukaan tavoitellaan virtualisoidusta prosessista poistumista sen isäntäympäristöön. Isäntäympäristöllä tarkoitetaan sitä ympäristöä, missä virtualisoitu prosessi alunperin käynnistettiin. Hyökkäyksen ajatuksena on, että hyökkääjä saisi samat oikeudet isäntäympäristössä, kuin millä itse virtualisoitu prosessi ajettiin. Nämä oikeudet voivat sisältää esimerkiksi ylläpitäjän oikeuksia, mahdollistaen lisähyökkäyksiä.

MITRE:n (2021d) mukaan palvelinpuolen pyynnönväärennös (CAPEC-664: *Server Side Request Forgery*) on hyökkäys, jossa hyökkääjä pyrkii saamaan palvelimen tekemään kutsun itseensä tai toiseen palveluun. Tällä hyökkääjä tavoittelee sitä, että kutsussa käytetään palvelimen oikeuksia, jotka voivat olla korkeammat kuin mitä hyökkääjän käyttäjällä itsellään on.

Viimeiseksi viidestä MITRE (2021e) lukee Bluetoothin avainneuvottelu hyökkäyksen (CAPEC-668: *Key Negotiation of Bluetooth Attack (KNOB)*). Hyökkäyksessä tarvitaan väliintulohyökkäystä, jonka avulla kuunnellaan laitteiden välistä Bluetooth-kommunikointia. Tämän jälkeen todentamisprosessin entropiabittejä muokataan, mahdollistaen viestien salauksen purkamisen.

3.3 Havaitseminen ja estäminen

OWASP (2021b) antaa esimerkkejä siitä, kuinka todentamisskeeman ongelmia voi syntyä eri vaiheissa kehitystä: esimerkiksi suunnitteluvaiheessa ei välttämättä huomioida, että jokin tietty asia tulisi piilottaa kirjautumisen taakse, toteutusvaiheessa syötteen validointi toteutetaan virheellisesti tai käyttöönotossa konfiguraatioon jää haavoittuvuuksia. Haavoittuvuuksien välttämiseksi on niiden havaitseminen sekä estäminen oleellisessa roolissa. Haavoittuvuuksia tulisi pyrkiä estämään hyvän ja perusteellisen suunnittelun avulla. Haavoittuvuudet, jotka syntyvät suunnittelusta huolimatta, olisi hyvä saada havaittua kehitysprosessin aikana niiden korjaamiseksi. Ne haavoittuvuudet, jotka eivät tule koko kehitysprosessin aikana havaituksi, voivat ennenpitkään tulla käytetyiksi hyökkäyksissä.

Suunnitteluvaiheessa on tärkeää valita järjestelmän kehittämiseen hyväksi todettuja ratkaisuja, kuten käyttää OWASP:in tarjoamaa todentamista (MITRE 2021g, s. 643). OWASP (2021a) ohjeistaa tunnistamisen ja todentamisen vikojen kategorian ongelmien välttämiseksi muun muassa monivaiheisen todentamisen käyttämistä, oletustunnuksien poistamista, heikkojen salasanojen tunnistamista, salasanan kompleksisuuden vaatimista tutkimustiedon pohjalta, virheviestien samanlaistamista järjestelmän tutkimisen estämiseksi viestien avulla, rajoittamaan sopivassa määrin toistuvia kirjautumisyrityksiä, lokittamaan kaikki oleelliset tiedot sekä käyttämään palvelinpuolen istunnonhallintaa huolellisesti hallitulla randomisoidulla tunnisteella. Väärän todentamisen alakategorioita on myös hyvä selata ymmärtääkseen

minkälaisia haavoittuvuuksia todentamiseen voi syntyä.

Väärän todentamisen haavoittuvuuksia voidaan havaita hyödyntäen esimerkiksi staattista analyysia sekä tarkastelemalla järjestelmän suunnitteludokumentteja (MITRE 2021g, s. 642–643). OWASP (2021b) ohjeistaa testaamaan todentamisen ohittamisen haavoittuvuuksilta eri tavoin käyttäen musta- tai harmaalaatikkotestausta. Mustalaatikkotestauksen avulla voi heidän mukaansa esimerkiksi testata päästääkö järjestelmä käyttäjän suoraan tiettyyn verkko-osoitteeseen tarkistamatta käyttäjää ja sen oikeuksia järjestelmässä tai huijaamalla todentamisen tapahtuneen osoitteen parametrien avulla. Mustalaatikkotestauksella voi myös kokeilla voiko järjestelmään tehdä injektiohyökkäyksen, kuten SQL-injektion. Lisäksi istuntojen tunnisteet voivat myös olla arvattavissa jonkin niissä esiintyvän kaavan kautta, näin mahdollistaen validin istuntotunnisteen helpomman arvaamisen. Mustalaatikkotestauksen lisäksi he tuovat esiin mahdollisuuden harmaalaatikkotestaukseen erityisesti jos koko ohjelmakoodi, tai osa siitä, on vapaasti tarjolla.

Haavoittuvuuksien havaitsemiseksi on kehitetty erilaisia työkaluja. Näistä kolme esimerkkiä ovat Firmalice, Nemesis ja EWVHunter. Firmalice on kehitetty löytämään todentamisen ohittamisen haavoittuvuuksia laiteohjelmistoista binääritasolla (Shoshitaishvili ym. 2015, s. 2). Nemesis taas löytää näitä haavoittuvuuksia verkkosovelluksista (Dalton, Kozyrakis ja Zeldovich 2009, s. 1), joissa OWASP pitää todentamisen ohittamista merkittävänä turvallisuusriskinä (OWASP 2021a). EWVHunteria voidaan käyttää oheislaitteissa todentamisen haavoittuvuuksien löytämiseen (Wang ym. 2020, s. 1).

4 Tutkimuskysymys

Todentamisen ohittamista yleisesti kuvaavaa tutkimusta vaikuttaa olevan rajallisesti. Tämän tutkimuksen tarkoituksena on täyttää tätä aukkoa aiheen tutkimuksessa kartoittamalla todentamisen ohittamiseen liittyvää tutkimusta ja antamalla kuvaa sen nykytilanteesta. Tämä tehdään seuraavan tutkimuskysymyksen kautta:

”Miten todentamisen ohittamista on tutkittu lähivuosina havaittuihin todentamisen ohittamisen haavoittuvuuksiin verrattuna?”

Tutkimuskysymystä tarkennetaan seuraavien lisäkysymysten kautta:

- Minkä tyyppisiä julkaisuja todentamisen ohittamisesta on tehty?
- Mitä todentamisen ohittamisen haavoittuvuuden tyyppejä julkaisuissa on tutkittu?
- Kuinka paljon todentamisen ohittamisen haavoittuvuuksia on havaittu samalla ajanjaksolla?
- Miten todentamisen ohittamisen haavoittuvuuden tyyppien esiintyvyys vertautuu niistä tehdyn tutkimuksen määrään?

5 Tutkimusmenetelmä

Tutkimus toteutetaan tekemällä systemaattinen kirjallisuuskartoitus. Kirjallisuuskartoituksen avulla voidaan kartoittaa aiheen tutkimuksen nykytilannetta hyödyntäen kategorisointia (Petersen ym. 2008, s. 1–2,7). Petersen ym. (2008, s. 2) kuvaa systemaattisen kirjallisuuskartoituksen prosessin viitenä vaiheena. On kuitenkin tärkeää huomata, että nämä prosessin vaiheet eivät välttämättä toteudu täysin lineaarisesti, vaan aiempia vaiheita voidaan hioa prosessin aikana uuden ymmärryksen pohjalta (Kitchenham ja Charters 2007, s. 6).

Prosessi lähtee liikkeelle tutkimuskysymyksen määrittelystä, jonka perusteella tutkimuksen laajuus määrittyy (Petersen ym. 2008, s. 2). Tämän tutkimuksen tutkimuskysymystä on kuvattu luvussa 4. Tämän jälkeen suoritetaan julkaisujen ja haavoittuvuuksien haku käyttäen suunniteltuja hakuja (Petersen ym. 2008, s. 3). Hakujen suunnittelua ja suorittamista esitellään luvuissa 6 ja 7. Hakujen perusteella saadut tulokset läpikäydään, jotta ainoastaan relevantit julkaisut ja haavoittuvuudet otetaan tutkimukseen mukaan (Petersen ym. 2008, s. 3).

Seuraavassa vaiheessa tulokset analysoidaan. Tulosten analysointi on kuvattu luvussa 8. Analysoinnissa relevantit julkaisut kategorisoidaan löytämällä aiheelle oleellisia avainsanoja (Petersen ym. 2008, s. 4). Lisäksi haavoittuvuudet kategorisoidaan hyödyntäen niiden hierarkkista rakennetta.

Viimeisenä vaiheena on tiedonpoiminta, jossa aiempaa kategorisointia hyödyntäen ja muovaten luodaan tutkimusaiheesta systemaattinen kartta (Petersen ym. 2008, s. 5). Tämä toimii tutkimuksen tuloksina ja se esitellään luvussa 9.

Tässä tutkimuksessa tutkimusmenetelmäksi on valittu systemaattinen kirjallisuuskartoitus, koska sen avulla voidaan läpikäydä laaja määrä julkaisuja tutkimuksen nykytilanteen kartoittamiseksi. Aiheeseen liittyy useita ala-alueita, joihin liittyvää analysointia voidaan esittää datan visualisoinnin kautta. Lisäksi julkaisujen kategorisointia voidaan vertailla muuhun dataan, kuten tässä tapauksessa haavoittuvuusdataan.

6 Aineiston keruun suunnittelu

Systemaattista kirjallisuuskartoitusta varten kehitetään arviointiprotokolla, jonka avulla tutkimusaineiston keruu toteutetaan. Lisäksi haavoittuvuuksiin vertaamista varten tulee löytää sopiva haavoittuvuuslistaus, jossa on dataa halutulta aikaväliltä.

Kirjallisuuskartoituksen käytännön toteutusta ajatellen julkaisuja tullaan hakemaan englanniksi, jotta aiheeseen löytyy mahdollisimman paljon tuoretta tutkimusta. Haku suoritetaan Jyväskylän yliopiston tunnusten kautta kirjautuneena. Julkaisujen valinta rajoittuu niihin julkaisuihin, jotka ovat avoimesti tarjolla luettavaksi tai Jyväskylän yliopiston lukuoikeuden alaisina. Julkaisujen tulee olla luettavissa kokonaisuudessaan englanniksi.

Käytettävien hakusanojen alustavassa suunnittelussa englanninkieliset termit ”*authentication*” eli todentaminen sekä ”*bypass*” eli ohittaminen tulisivat todennäköisesti tuottamaan tuloksia, sillä näitä termejä esiintyy laajasti aiheeseen liittyvissä teksteissä. Hakutermien odotetaan löytyvän julkaisujen metadatasta.

Hakutermien kohdalla tulee huomata, että termit voivat esiintyä eri järjestyksissä ja muodoissa, esimerkiksi ”*authentication bypass*” sekä ”*bypassing authentication*”. Haussa termien järjestyksen tulee olla vapaa, sekä hakusanoissa on hyvä käyttää jokerimerkkiä. Jälkimmäisellä tarkoitetaan sitä, että käytetään esimerkiksi hakutermiä ”*authenticat**” mahdollistamaan hakutuloksissa sekä ”*authenticat**ion***” että ”*authenticat**ing***”.

Tutkimuksen nykyhetkeä ajatellen haun ajallinen rajoitus on viimeiset kolme kokonaista vuotta (2019-2021), jotta tutkimus on tarpeeksi tuoretta. Tutkimukseen valittiin vain kokonaisia vuosia selventämään tutkimukseen mukaanluettua dataa.

Aikarajauksen perusteella valitaan myös haavoittuvuuslistauksia samoilta vuosilta vertailun kohteeksi. Haavoittuvuuksien kohdalla voidaan hyödyntää haavoittuvuuslistauksen hierarkista rakennetta valitsemaan tutkimukseen mukaan ne haavoittuvuudet, jotka liittyvät väärään todennukseen tai sen alakategorioihin.

7 Aineiston keruu

Todentamisen ohittamiskeinoihin liittyvät julkaisut kerättiin arviointiprotokollan mukaisesti. Julkaisujen haku suoritettiin Jyväskylän yliopiston tunnuksilla kirjautuneena tutkimuksien hakemiseen tarkoitetuissa Scopus ja IEEE Xplore -palveluissa. Julkaisut haettiin 31.1.2022.

Haavoittuvuuslistauksia on vapaasti ladattavissa NIST NVD-sivustolta (*National Institute of Standards and Technology*: *National Vulnerability Database*) (NIST 2021). Sieltä tutkimukseen valittiin haavoittuvuuslistaukset saman aikarajauksen mukaan kuin julkaisut, eli vuosilta 2019–2021.

Haavoittuvuuslistauksia käytettäessä on hyvä huomata, että haavoittuvuusdataa saatetaan muokata jälkikäteen. Tämän takia tutkimuksen kannalta on tärkeää tallentaa datasta tietty versio tutkimuksen ajan käytettäväksi. Tutkimusta varten haavoittuvuuslistaus haettiin 31.1.2022.

8 Aineiston analysointi

Kaikki hakujen avulla löytyneet julkaisut dokumentoitiin. Kaikki julkaisut löytyvät liitteestä A. Julkaisuista karsittiin pois ne, jotka eivät liittyneet tutkittavaan aiheeseen. Hylätyistä julkaisuista dokumentoitiin hylkäyksen syy.

Hyväksytyistä julkaisuista arvioitiin minkä tyyppisiä tutkimukset ovat sekä mihin todentamisen ohittamisen haavoittuvuuden luokkaan ne liittyvät, luokitellen ne väärän todennuksen (CWE-287) haavoittuvuuksien alaluokitusten mukaisesti. Julkaisun liittyessä aiheeseen, mutta ei tarkemmin minkään alaluokituksen alle, se luokitellaan suoraan pääluokan alle. Luokituksessa noudatettiin tällä hetkellä uusinta julkaistua CWE-versiota 4.6.

Julkaisuista päätettiin kirjata ylös myös niiden aihe, jakaen ne sen avulla aihepiireittäin. Tämä tehtiin antamaan lisää kuvaa minkälaisia asioita todentamisen ohittamisen tutkimuksissa käsitellään. Tarkemmin julkaisujen luokitteluista ja tuloksista esitellään luvussa 9.1.

Haavoittuvuuslistauksista etsittiin relevantit haavoittuvuudet ensisijaisesti niiden sisältämien haavoittuvuusluokitusten perusteella. Haavoittuvuudet luokiteltiin haavoittuvuusluokitusten hierarkkista rakennetta ylöspäin kulkien väärän todennuksen alaluokkiin. Haavoittuvuus voitiin luokitella myös pelkästään pääluokan alaiseksi, jos haavoittuvuus oli suorassa linkissä pääluokkaan, mutta ei sen alaluokkiin.

Kaikissa haavoittuvuuksissa ei kuitenkaan ollut merkittynä haavoittuvuusluokituksia, vaan sen sijaan merkintä ”NVD-CWE-noinfo”. Tämä voi johtua esimerkiksi siitä, että hyvin tuoreissa haavoittuvuuksissa voi olla rajallisesti tietoja täytettynä. Näiden löytämiseksi käytettiin lisäksi toissijaista hakua haavoittuvuuden kuvauksesta. Haku tehtiin käyttäen samoja termejä kuin julkaisujen yhteydessä: ”*authenticat**” ja ”*bypass**”. Nämä luokiteltiin manuaalisesti saman kaavan mukaisesti väärän todennuksen alaluokkien tai itse pääluokan alle. Jos haavoittuvuus ei kuvauksen perusteella liittynyt todentamisen ohittamiseen, se hylättiin.

Manuaalisesti luokitellut haavoittuvuudet löytyvät liitteestä B. Kaikki tutkimukseen mukaanotetut väärän todennuksen alaiset haavoittuvuudet – niin hierarkkisesti kuin manuaalisesti jaetut – löytyvät liitteestä C. Haavoittuvuuksiin liittyviä tuloksia ja yksityiskohtia käsitellään

luvussa 9.2.

Tutkimuksen tavoitteena on tarkastella tutkimuksen nykytilannetta. Haavoittuvuuksista ja julkaisuista selvitettiin, kuinka paljon minkäkin luokituksen edustajaa löydettiin tutkittavina vuosina. Väärän todennuksen alaluokkien pohjalta tehdyn kategorisoinnin perusteella voitiin arvioida missä suhteessa erityyppisiä todentamisen ohittamiskeinoja on tutkittu ja niistä löydetty haavoittuvuuksia tutkitulla aikavälillä. Vertailuun liittyvät tulokset esitellään luvussa 9.3.

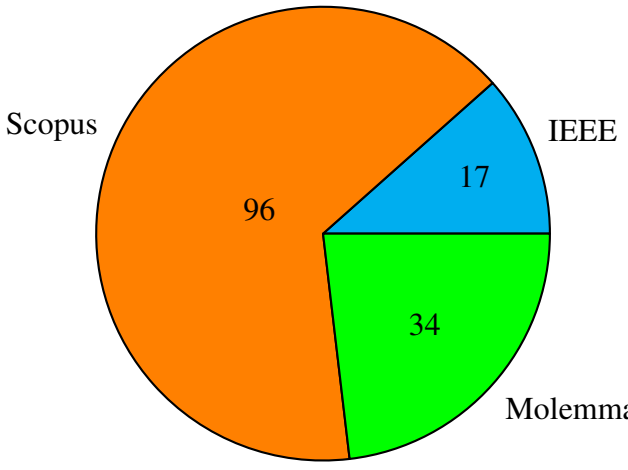
9 Tulokset

Tuloksien käsittely on jaettu kolmeen osaan. Luvussa 9.1 käsitellään julkaisujen analysoinnin tulokset. Luvussa 9.2 esitellään väärän todennuksen haavoittuvuuksiin liittyvät tulokset. Julkaisuista ja haavoittuvuuksista saatuja tuloksia vertaillaan luvussa 9.3. Lopuksi luvussa 9.4 käydään läpi pohdintaa tutkimukseen liittyen.

9.1 Julkaisut

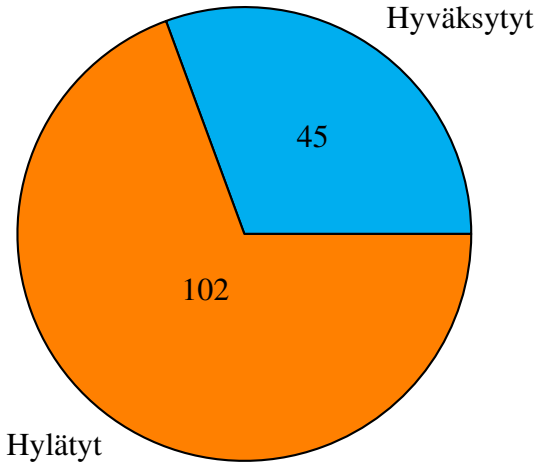
Julkaisuihin liittyvät tulokset esitellään seuraavassa järjestyksessä. Ensin käydään läpi miten tutkimukseen hyväksytyt julkaisut löydettiin. Tähän kuuluu löydettyjen julkaisujen lukumäärä tietokannoittain sekä hyväksyttyjen ja hylättyjen julkaisujen suhde. Tämän jälkeen esitellään hyväksyttyjen julkaisujen jako tyypityksen, kategorisoinnin sekä aiheen perusteella. Samalla tuodaan esille julkaisujen jakoa vuosittaisella tasolla.

9.1.1 Hyväksytyt



Kuvio 1. Löydettyjen julkaisujen määrä tietokannoittain

Julkaisujen haku suoritettiin suunnitellusti kahdessa eri tietokannassa – IEEE ja Scopus. IEEE:stä haulla löytyi 51 ja Scopuksesta 130 julkaisua. Yhteensä julkaisuja löytyi 147. Näistä 34 löytyi molemmista tietokannoista. Hauilla löytyneiden julkaisujen määrät on esitetty



Kuvio 2. Hyväksyttyjen ja hylättyjen julkaisujen suhde

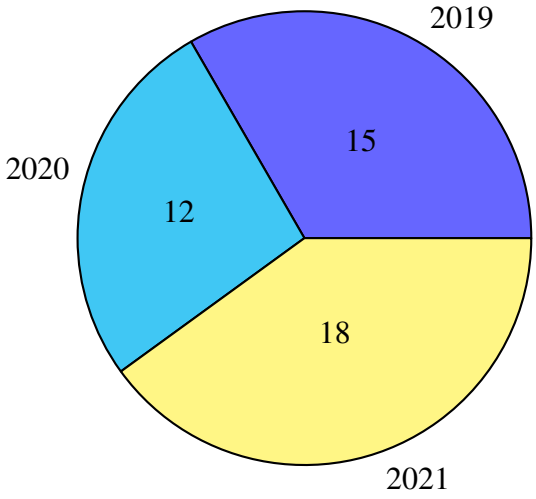
tietokannoittain kuviossa 1. Kaikki hauilla löytyneet julkaisut löytyvät liitteestä A.

Julkaisuista 45 hyväksyttiin tutkimukseen. Tämä on noin 30% kaikista hauilla löydetyistä julkaisuista. Hylättyjä julkaisuja oli 102. Hyväksyttyjen ja hylättyjen julkaisujen suhde on esitetty kuviossa 2. Liitteessä A on selitetty hylkäyssyy kaikille hylätyille julkaisuille.

Julkaisuista hylättiin pois ne, jotka eivät täyttäneet luvussa 6 esiteltyä ehtoa: julkaisujen tuli olla kokonaisuudessaan englanninkielellä saavutettavissa joko avoimesti tai Jyväskylän yliopiston lukuoikeuden alaisena. Lisäksi yksi julkaisu hylättiin, koska se ei ollut yksittäinen julkaisu, vaan kokoelma. Muista julkaisuista hyväksyntä tehtiin julkaisun tekstin pohjalta.

Tutkimukseen hyväksyttiin todentamisen ohittamista käsittelevät julkaisut. Tutkimuksesta hylättiin sellaiset julkaisut, joissa käsitellään vain todentamista, mutta ei todentamisen ohittamista joko lainkaan tai se mainitaan vain lyhyesti sivussa. Tällöin esimerkiksi julkaisut, joissa todentamisen ohittamista käsitellään ainoastaan julkaisun aiheen esittelyssä, rajattiin tutkimuksen ulkopuolelle.

Julkaisuista hylättiin myös tapaukset, joissa todentamisen ohittamiseen liittyen todetaan, ettei todentamista ole järjestelmässä käytössä tai esiehtona on oletus että todentaminen on jo ohitettu. Jälkimmäisessä tapauksessa hyväksyttiin kuitenkin tilanteet, joissa tutkimus käsittelee todentamisen ohittamista monivaiheisessa todentamisessa, jonka vaiheista osa on esiehtona ohitettu.



Kuvio 3. Julkaisujen lukumäärä vuosittain

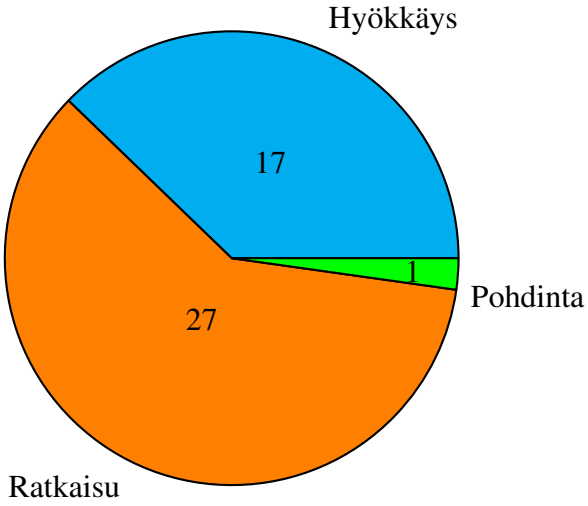
Hyväksytyt julkaisut voidaan jakaa niiden julkaisuvuosien perusteella tutkittaviin vuosiin 2019, 2020 ja 2021. Vuositasolla julkaisujen määrä jakautui hyvin tasaisesti. Julkaisut on esitetty vuosittain kuviossa 3.

9.1.2 Tyypitys

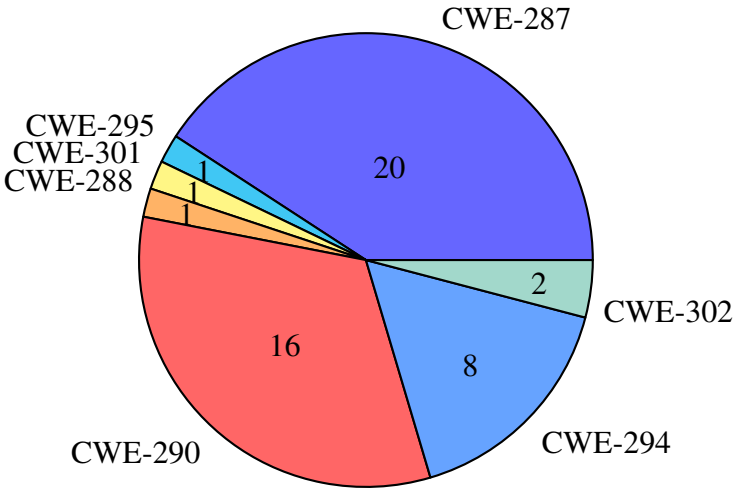
Hyväksytyistä julkaisuista määritettiin tyyppi sen perusteella miten julkaisuissa käsiteltiin todentamisen ohittamista. Hyväksytyt julkaisut jaettiin tyyppeihin hyökkäys, pohdinta ja ratkaisu. Moni julkaisuista sisältää useampaa näistä, mutta julkaisut on jaettu tyyppeihin niiden pääpainotuksen perusteella.

Hyökkäystyyppisissä julkaisuissa pääasiassa kuvataan ja toteutaan todentamisen ohittamisen haavoittuvuuteen kohdistettu hyökkäys. Pohtivissa julkaisuissa taas painotus on jonkin todentamisen ohittamiseen liittyvän ilmiön kuvaamisessa yleisemmällä tasolla. Ratkaisupainotteisissa julkaisuissa julkaisun tärkein kontribuutio on siinä kuvattu ratkaisu, jolla voidaan vähentää todentamisen ohittamisen haavoittuvuuksia.

Julkaisuista suurin osa kuvasi ratkaisuja. Ratkaisupainotteisten lisäksi hyökkäyksiä kuvaavia julkaisuja oli myös iso osa julkaisuista. Pohdintaan keskittyviä julkaisuja oli hyväksytyissä julkaisuissa vain yksi. Julkaisujen määrät on kuvattu tyypeittäin kuviossa 4.



Kuvio 4. Julkaisujen lukumäärä tyypeittäin



Kuvio 5. Julkaisuista nousseiden kategorioiden lukumäärät

9.1.3 Kategorisointi

Julkaisut kategorisoitiin julkaisun tekstin perusteella väärän todennuksen ja sen alakategorioiden alle. Kuten luvussa 3.1.2 todettiin, väärä todennus (CWE-287) sisältää seuraavat alakategoriat:

- CWE-261: Heikko salasanan koodaus
- CWE-262: Salasanan vanhenemisen puute
- CWE-263: Salasanan vanheneminen pitkällä erääntymisajalla

- CWE-288: Todentamisen ohittaminen käyttämällä vaihtoehtoista reittiä tai kanavaa
- CWE-289: Todentamisen ohittaminen käyttämällä vaihtoehtoista nimeä
- CWE-290: Todentamisen ohittaminen huijaamalla
- CWE-294: Todentamisen ohittaminen toiston avulla
- CWE-295: Sopimaton sertifikaatin validointi
- CWE-301: Reflektiohyökkäyksen mahdollisuus todennusprotokollassa
- CWE-302: Todentamisen ohittaminen muuttumattomaksi oletetun datan avulla
- CWE-303: Sopimaton todentamisalgoritmin toteutus
- CWE-304: Kriittisen vaiheen puute todentamisesta
- CWE-305: Todentamisen ohittaminen ensisijaisen heikkouden avulla
- CWE-306: Todentamisen puute kriittisestä funktiosta
- CWE-307: Sopimaton rajoitus liiallisille todentamisyrityksille
- CWE-308: Yksivaiheisen todentamisen käyttäminen
- CWE-309: Salasanan käyttäminen pääasiallisena todentamisen tapana
- CWE-521: Heikot salasanan vaatimukset
- CWE-522: Vajaasti suojellut tunnukset
- CWE-593: Todentamisen ohittaminen muuttamalla OpenSSL CTX-objektia SSL-objektien luonnin jälkeen
- CWE-603: Todentamisen suorittaminen käyttäjäpuolella
- CWE-620: Varmistuksen puute salasananvaihdossa
- CWE-640: Heikko unohdetun salasanan palautusmekanismi
- CWE-645: Liikaa rajoittava käyttäjän lukitusmekanismi
- CWE-798: Kovakoodattujen tunnusten käyttö
- CWE-804: Arvattava CAPTCHA
- CWE-836: Todentamisessa salasanatiivisteen käyttö salasanan sijaan

Kategorisointi tehtiin sen perusteella minkälainen todentamisen ohittamiseen liittyvä haavoittuvuus julkaisussa esitetyssä tilanteessa oli kyseessä näitä kategorioita ajatellen. Kategorisoinnissa julkaisulle voitiin antaa joko yksi tai useampi kategoria. Tällöin haavoittuvuus liittyi useampaan kategoriaan tai julkaisussa käsiteltiin useampaa erilaista haavoittuvuutta.

Kaikkien erilaisten käsiteltyjen haavoittuvuuksien kohdalla ei ollut yksinkertaista määrit-

Kategoria	2019	2020	2021	Yhteensä
CWE-287	9	4	7	20
CWE-290	3	6	7	16
CWE-294	2	2	4	8
CWE-302	1	1	0	2
CWE-295	1	0	0	1
CWE-288	1	0	0	1
CWE-301	0	1	0	1

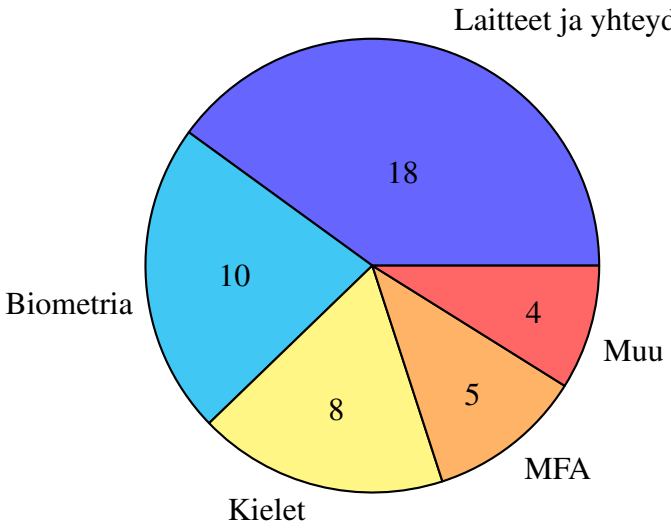
Taulukko 1. Julkaisuista nousseiden kategorioiden lukumäärät jaettuna vuosittain

tää mihin alakategoriaan ne kuuluvat. Tällaisissa tilanteissa julkaisuille voitiin myös antaa väärän todennuksen pääluokka tarkemman alaluokan sijaan. Esimerkiksi SQL-injektioihin liittyviä julkaisuja oli useita, mutta väärän todentamisen alla ei ole suoraan niihin selkäesti viittaavaa alaluokkaa. Väärään todennukseen liittyen MITRE (2021g, s. 645) kuitenkin mainitsee todentamisen voivan olla haavoittuvainen SQL-injektiohaavoittuvuuksien takia.

Suoraan pääluokan (CWE-287) alle kategorisoituja julkaisuja oli yhteensä 20. Nämä edustivat suurinta osuutta julkaisujen kategorioista. Toiseksi eniten käsiteltiin huijaukseen perustuvia todentamisen ohittamisen haavoittuvuuksia ja kolmanneksi eniten toiston kautta tehtävää todentamisen ohittamista. Julkaisuissa oli myös vähemmällä tasolla alakategorioita liittyen todentamisen ohittamiseen muuttumattomaksi oletetun datan avulla (CWE-302) sekä vaihtoehtoisen reitin tai kanavan käytön kautta (CWE-288), sekä liittyen sopimattomaan sertifikaatin validointiin (CWE-295) ja reflektiohyökkäyksen mahdollisuuteen todennusprotokollassa (CWE-301). Kaikki julkaisuista nousseet kategoriat on esitetty kuviossa 5.

Kategorisointia ajatellen tulee huomioida, että julkaisujen haku tehtiin todentamisen ohittamista ajatellen. Näin kategorisoinnissa korostuvat nimenomaan todentamisen ohittamiseen eniten liittyvät väärän todennuksen alakategoriat.

Julkaisut voidaan jakaa edelleen kategorioiden sekä julkaisuvuosien perusteella. Taulukossa 1 on esitetty miten väärä todennus ja sen alakategoriat on edustettuina julkaisuissa vuosittaisella tasolla. Kategorioiden rajallisen edustajamäärän takia jaottelusta ei voi tehdä juuri-



Kuvio 6. Julkaisujen lukumäärä aiheittain

kaan johtopäätöksiä. Selkein muutos voidaan nähdä huijaukseen perustuvien todentamisen ohittamisen haavoittuvuuksien (CWE-290) käsittelyssä. Niiden määrä on kasvanut jokaisen tutkittavan kolmen vuoden aikana.

9.1.4 Aiheittain

Aiemmin esitelty tyypitys antaa kuvaa julkaisun tavoitteesta ja kategorisointi kuvaa yleisemmällä tasolla minkälaisia haavoittuvuuksia julkaisussa käsitellään. Näiden lisäksi päätin kirjoittaa hyväksytyistä julkaisuista ylös niissä esiintyviä aihealueita samanlaisuuksien löytämiseksi. Aiheittaisen jaottelun avulla pyritään laajentamaan kuvaa siitä minkälaisia asioita julkaisuissa käsitellään.

Kuviossa 6 on esitelty julkaisujen jako aiheittain. Jokainen julkaisu on määritetty edustamaan yhtä aihetta. Laitteisiin ja yhteyksiin liittyviä julkaisuja oli kaikista eniten. Näihin mukaanlukeutuivat esimerkiksi laitteiden väliseen todentamiseen liittyvät julkaisut.

Toiseksi isoimpana kategoriana olivat biometriseen todentamiseen liittyvät julkaisut. Julkaisuissa käsiteltiin useita erilaisia tapoja todentaa biometrisesti, kuten sormenjäljen, iiriksen, kävelytyylin ja kasvojen tunnistamisen kautta. Biometriseen todentamiseen liittyvissä julkaisuissa nostettiin usein esiin myös esimerkiksi eloisuuden (engl. *liveness*) tarkistaminen

Vuosi	Väärä todennus	Kaikki	Osuus
2019	1014	16512	$\approx 6,1\%$
2020	1127	19128	$\approx 5,9\%$
2021	900	17715	$\approx 5,0\%$
Yhteensä	3041	53355	$\approx 5,7\%$

Taulukko 2. Väärän todennuksen osuus kaikista raportoiduista haavoittuvuuksista

todentamisen huijaamisen estämiseksi.

Kielten aiheeseen luettiin mukaan julkaisut, joissa käsiteltiin ohjelmointiin liittyvien kielten ominaisuuksia. Tällaisia ovat esimerkiksi SQL-injektioihin sekä ohjelmointikielten tyypitykseen liittyvät julkaisut.

Monivaiheiseen todentamiseen liittyviä julkaisuja oli 5. Nämä on eroteltuna biometrisen todentamisen aiheesta, sillä näissä julkaisuissa aiheena oli enemmänkin todentamisen monivaiheisuus kuin se, minkälainen todentaminen missäkin vaiheessa on käytössä.

Loput julkaisut, jotka eivät sopineet muiden julkaisujen kanssa samaan aihepiiriin, laitettiin luokkaan ”muu”. Muiden aiheiden luokassa julkaisuissa käsiteltiin tuotteiden viivakoodin väärentämistä, todentamisen protokollasta kolmannen osapuolen tarkistuksen poistamiseen, kryptografian kvanttiresistenssiä sekä paluuosoitehyökkäyksiä.

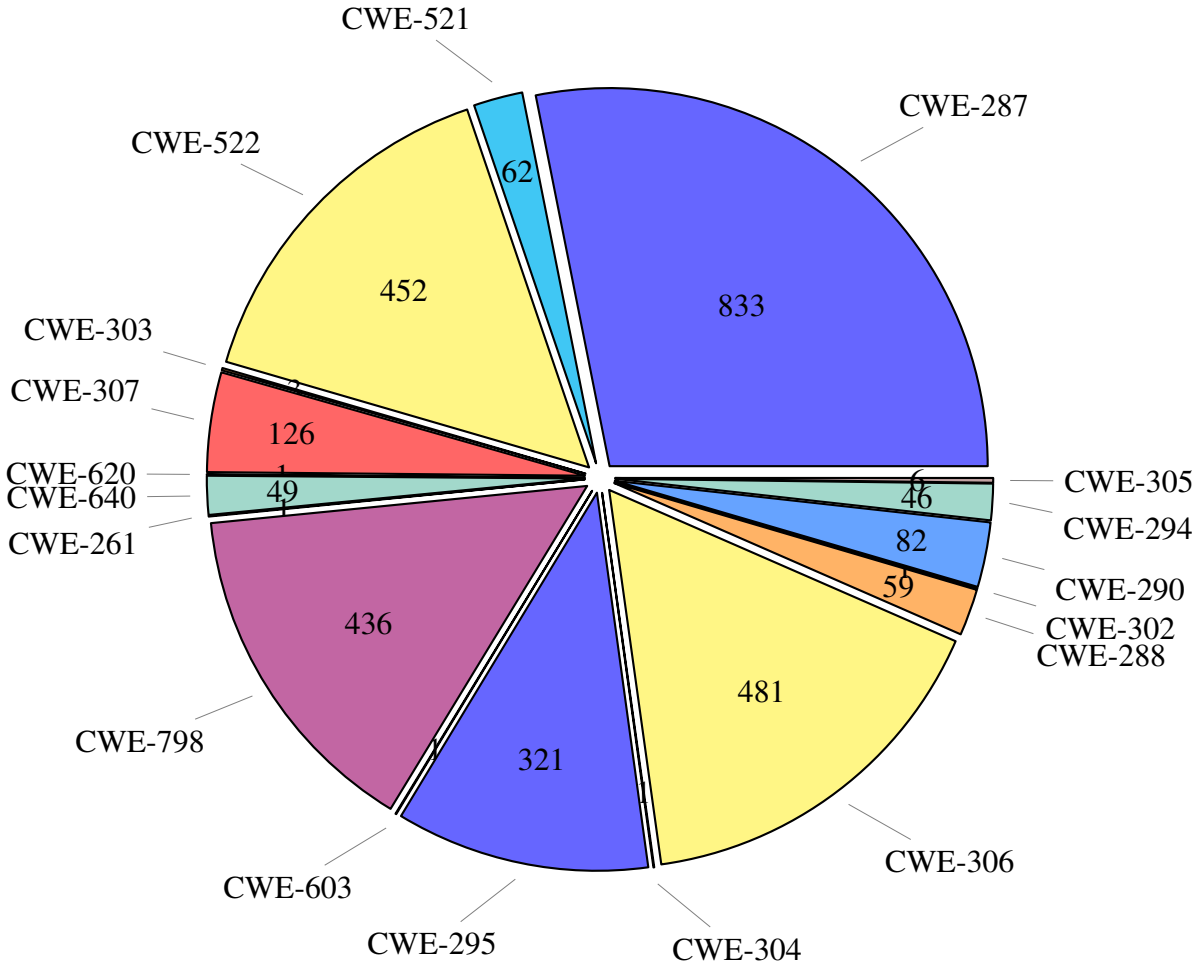
9.2 Haavoittuvuudet

Haavoittuvuuksiin liittyvät tulokset käydään läpi seuraavasti: ensin käydään läpi haavoittuvuusluokituksen sisältävät haavoittuvuudet, jotka jaettiin hierarkkisesti väärän todentamisen kategorioihin. Toiseksi esitellään haavoittuvuudet, joista haavoittuvuusluokitus puuttui. Nämä jaettiin käsin kuvauksen pohjalta samoihin kategorioihin. Näiden käsittelemisen jälkeen tuodaan esiin tulokset liittyen kaikkiin löydettyihin haavoittuvuuksiin.

9.2.1 Hierarkkisesti jaetut

Taulukossa 2 on esitetty väärään todentamiseen ja sen alakategorioihin linkittyvät haavoittuvuudet suhteessa kaikkiin haavoittuvuuksiin. Linkkiin hyväksytään kolmen polven aikana väärän todennuksen kategoriaan linkittyvät haavoittuvuudet.

Väärän todennuksen ja sen alakategorioiden alaisia haavoittuvuuksia oli kaikkina hakuvuosina yhteensä 3041. Tämä on noin 5,7 prosenttia kaikista haavoittuvuuksista. Väärän todennuksen osuus kaikista haavoittuvuuksista on vaihdellut vuosittain 5,0 – 6,1% välillä.



Kuvio 7. Väärän todennuksen haavoittuvuudet hierarkian perusteella kategorioittain

Haavoittuvuusluokituksen omaavat haavoittuvuudet voitiin jakaa haavoittuvuusluokitusten hierarkkista rakennetta käyttäen lähimpään kategoriaansa. Näistä suurin osa linkittyi suoraan pääluokkaan. Pääluokan alle on luokiteltu ne, jotka ovat lähimpänä yläluokkaa alaluokkien

sijaan.

Pääluokan lisäksi iso osa haavoittuvuuksista kuului kriittisestä funktiosta todentamisen puuttumisen (CWE-306), vajaasti suojeltujen tunnusten (CWE-522), kovakoodattujen tunnusten käytön (CWE-798) tai sopimattoman sertifikaatin validoinnin (CWE-295) alle. Haavoittuvuuksien jakautuminen on esitetty kuviossa 7.

9.2.2 Manuaalisesti jaetut

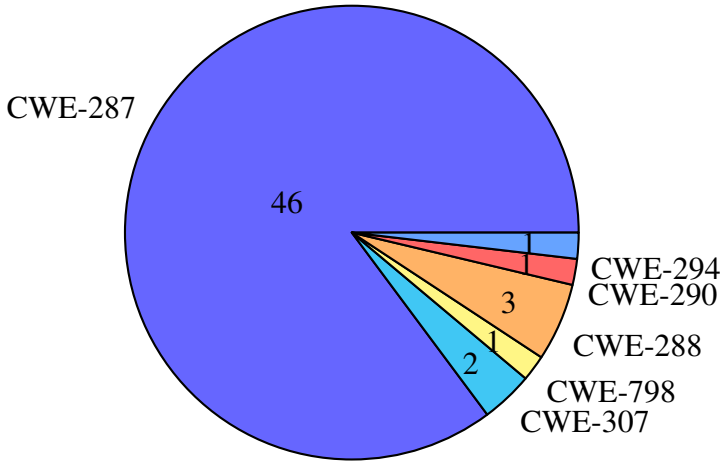
Osasta haavoittuvuuksista puuttuu haavoittuvuusluokitus – näistä haettiin haavoittuvuuksia tutkimusta varten käyttäen termihakua haavoittuvuuksien kuvauksissa. Termihaussa käytetyt termit esitettiin luvussa 8. Hakutermit ovat kuitenkin tarkoitettu löytämään todentamisen ohittamiseen liittyviä tuloksia, joten löydetyt haavoittuvuudet eivät edusta kaikkia luokittelemattomia haavoittuvuuksia koko väärään todennukseen liittyen.

Osa haavoittuvuuksista hylättiin, sillä ne eivät kuvauksen perusteella vaikuttaneet liittyvän todentamiseen, vaan esimerkiksi valtuutuksen ongelmiin. Liitteessä B on esitettynä kaikki manuaalisesti luokitellut haavoittuvuudet, mukaanlukien tutkimuksesta hylätyt haavoittuvuudet.

Yllättäen haavoittuvuuksia löydettiin termihaulla eniten käänteisessä järjestyksessä haavoittuvuuden tuoreuteen nähden. Lisäksi vuodelta 2021, jolta haavoittuvuuksia löytyi vähiten, löytyi ainoastaan yksi haavoittuvuus. Haavoittuvuuksista olisi voinut ajatella, että uudempiin haavoittuvuuksiin ei olisi lisätty vielä kaikkia tietoja. Nämä tulokset eivät kuitenkaan viittaa tähän. Termihaulla löydettyjen hyväksyttyjen haavoittuvuuksien määrä vuosittain on esitetty taulukossa 3.

Vuosi	**Määrä**
2019	37
2020	15
2021	1
Yhteensä	53

Taulukko 3. Manuaaliset jaetut haavoittuvuudet vuosittain



Kuvio 8. Termihaun avulla löydetyt haavoittuvuudet, joilta puuttuu hierarkkinen kategorisointi, manuaalisesti jaettuna kategorioihin.

Termihaun avulla löytyneet haavoittuvuudet jaettiin kuvauksen perusteella kategorioihin. Tämä on esitetty kuviossa 8. Luokittelemattomien haavoittuvuuksien kategorisoinnissa jos mikään alakategoria ei selkeästi kuvannut haavoittuvuutta, haavoittuvuus luokiteltiin suoraan pääluokan alle. Tämä oli yleistä, sillä monissa haavoittuvuuksissa kuvaus oli hyvin lyhyt ja epätarkka, vaikeuttaen tarkemman kategorisoinnin tekemistä.

9.2.3 Kaikki haavoittuvuudet

Seuraavaksi käsitellään kaikkia löydettyjä haavoittuvuuksia – niin hierarkkisesti löydettyjä kuin termihausta hyväksyttyjä haavoittuvuuksia. Haavoittuvuuksien joukossa oli 9 haavoittuvuutta, jotka linkittyivät useampaan väärän todennuksen alakategoriaan. Nämä haavoittuvuudet löytyvät taulukosta 4. Väärän todennuksen yläkategoriaan linkittymistä alakategorian lisäksi ei lasketa tähän mukaan, sillä jokainen haavoittuvuus linkittyisi sekä ylä- että alakategoriaan, ellei kolmen polven rajoite estäisi sitä.

Tutkimukseen hyväksyttyjä haavoittuvuuksia oli yhteensä 3094. Tämä on noin 5,8 prosenttia kaikista haavoittuvuuksista tutkittujen vuosien ajalta. Haavoittuvuuksien jakaantuminen tutkituille vuosille on esitetty taulukossa 5. Haavoittuvuudet ovat jakautuneet melko tasaisesti tutkittujen vuosien ajalle. Osuus kaikista haavoittuvuuksista on vuosittain vaihdellut 5,0 – 6,4% välillä, joka on hieman enemmän kuin pelkästään hierarkkisesti jaettujen haa-

#	CVE	Kategoriat
1	CVE-2019-14927	CWE-288, CWE-306
2	CVE-2019-15655	CWE-306, CWE-522
3	CVE-2019-9733	CWE-290, CWE-798
4	CVE-2020-28937	CWE-288, CWE-306
5	CVE-2020-2033	CWE-290, CWE-295
6	CVE-2020-8790	CWE-307, CWE-521
7	CVE-2020-9306	CWE-522, CWE-798
8	CVE-2021-41028	CWE-295, CWE-798
9	CVE-2021-28912	CWE-521, CWE-798

Taulukko 4. Useammassa väärän todennuksen alakategoriassa olevat haavoittuvuudet

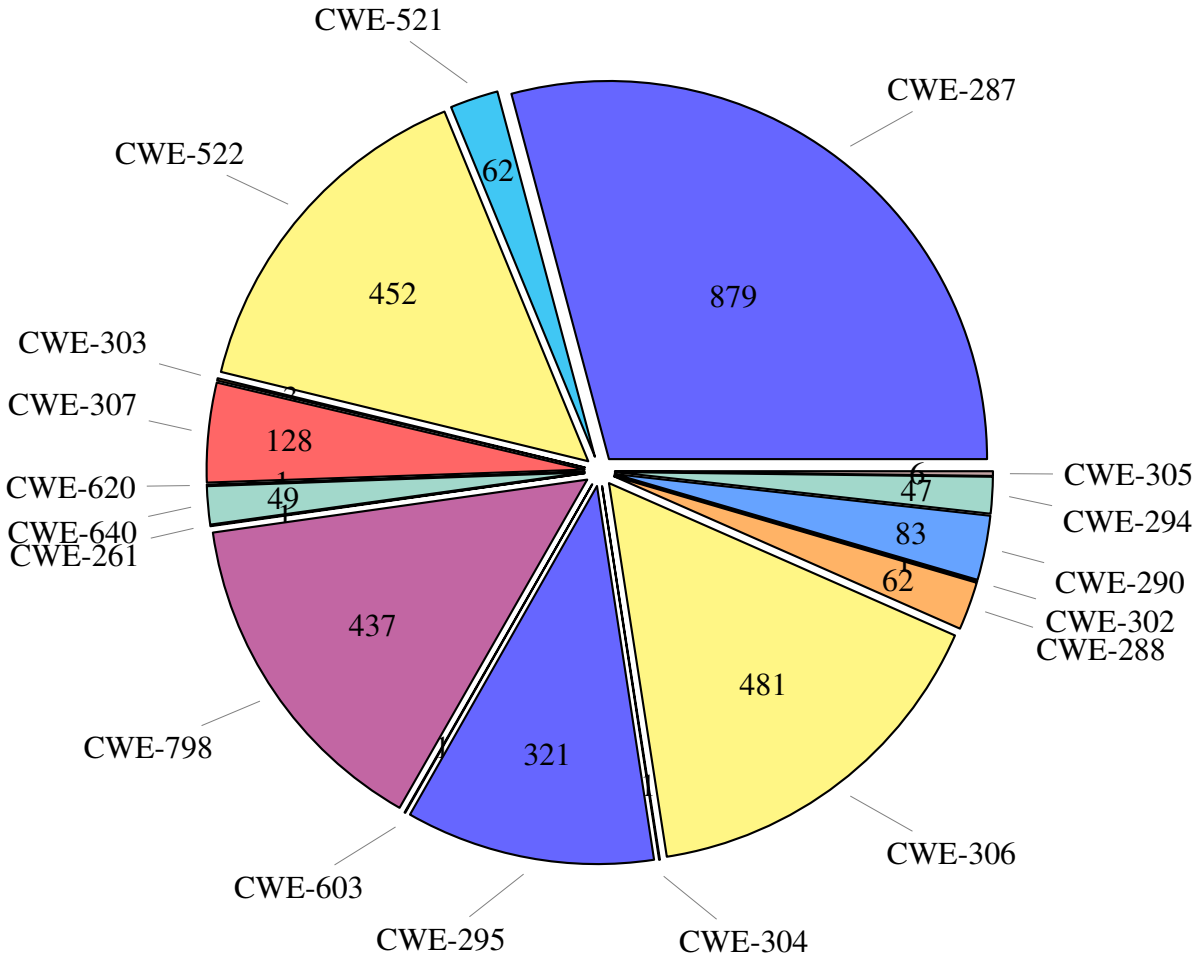
Vuosi	Määrä	Kaikki	Osuus
2019	1051	16512	$\approx 6,4\%$
2020	1142	19128	$\approx 6,0\%$
2021	901	17715	$\approx 5,0\%$
Yhteensä	3094	53355	$\approx 5,8\%$

Taulukko 5. Kaikki haavoittuvuudet vuosittain

voittuvuuksien kohdalla. Tämä johtuu siitä, että termihaun kautta vuodelle 2021 tuli vain yksi haavoittuvuus lisää.

Kategorisoinnin näkökulmasta haavoittuvuuksien jakautuminen kategorioihin pysyi hyvin tasaisena – termihaulla löytyneiden haavoittuuvuksien lisääminen hierarkkisesti löydettyjen haavoittuvuuksien mukaan ei tuonut juurikaan eroja kategorioiden määrien suhteisiin. Kaikki tutkimukseen hyväksytyt haavoittuvuudet on esitetty kategorioittain kuviossa 9, jossa on kuvioiden 7 ja 8 data yhdistettynä.

Haavoittuvuuksista suurin osa oli edelleen pääluokan edustajia. Pääluokan lisäksi haavoittuvuuksia löytyi paljon liittyen alakategorioihin todentamisen puutteesta kriittisestä funktiosta (CWE-306), vajaasti suojelluista tunnuksista (CWE-522), kovakoodattujen tunnusten käytöstä (CWE-798), sopimattomasta sertifikaatin validoinnista (CWE-295) ja sopimattomasta



Kuvio 9. Kaikki haavoittuvuudet kategorioittain

rajoituksesta liiallisille todentamisyrityksille (CWE-307).

Näiden jälkeen seuraavaksi eniten haavoittuvuuksia on kategorioissa todentamisen ohittaminen huijaamalla (CWE-290), heikot salasanan vaatimukset (CWE-521), todentamisen ohittaminen käyttämällä vaihtoehtoista reittiä tai kanavaa (CWE-288), heikko unohdetun salasanan palautusmekanismi (CWE-640) ja todentamisen ohittaminen toiston avulla (CWE-294). Loput haavoittuvuudet menevät kategorioihin todentamisen ohittaminen ensisijaisen heikkouden avulla (CWE-305), sopimaton todentamisalgoritmin toteutus (CWE-303), todentamisen ohittaminen muuttumattomaksi oletetun datan avulla (CWE-302), varmistuksen puute salasananvaihdossa (CWE-620), kriittisen vaiheen puute todentamisesta (CWE-304), heikko salasanan koodaus (CWE-261) ja todentamisen suorittaminen käyttäjäpuolella (CWE-603).

Kategoria	2019	2020	2021	Yhteensä
CWE-287	239	282	358	879
CWE-306	215	215	51	481
CWE-522	188	150	114	452
CWE-798	125	173	139	437
CWE-295	94	129	98	321
CWE-307	31	53	44	128
CWE-290	27	30	26	83
CWE-288	33	22	7	62
CWE-521	22	23	17	62
CWE-640	16	10	23	49
CWE-294	11	22	14	47
CWE-305	1	3	2	6
CWE-303	0	1	2	3
CWE-261	0	1	0	1
CWE-603	0	1	0	1
CWE-302	0	0	1	1
CWE-304	0	0	1	1
CWE-620	0	0	1	1

Taulukko 6. Haavoittuvuuksien edustus kategorioissa vuosittain

Vuosittaisella tasolla kategorioiden esiintymät kaikissa tutkimukseen hyväksytyissä julkaisuissa on esitetty taulukossa 6. Pääluokkaa (CWE-287) edustavien haavoittuvuuksien määrä on tutkittujen vuosien aikana ollut selkeässä nousussa. Päinvastoin CWE-522 liittyen vajaasti suojeltuihin tunnuksiin on ollut laskussa. Laskua on havaittavissa myös vaihtoehtoisen reitin tai kanavan käytössä todentamisen ohittamiseksi (CWE-288). Kriittisissä funktioissa todentamisen puuttumisen (CWE-306) kohdalla taas vuosina 2019 ja 2020 lukumäärät pysyivät samana, mutta 2021 niitä havaittiin huomattavasti vähemmän.

9.3 Vertailu

Julkaisujen ja haavoittuvuuksien edustukset kaikissa väärän todennuksen kategorioissa on koottu taulukkoon 7. Samassa taulukossa on esitettynä myös jako vuosittaisella tasolla.

Niin julkaisuissa kuin haavoittuvuuksissa suurin osa oli pääluokan edustajia. Julkaisuissa esiintyneet kategoriat olivat edustettuina myös haavoittuvuuksissa, lukuunottamatta reflektiohyökkäyksen mahdollisuutta todennusprotokollassa (CWE-301).

Julkaisuista ja haavoittuvuuksista saatuja tuloksia vertaillessa tulee huomioida, että hierarkkisesti haavoittuvuuksia haettiin koko väärän todennuksen alueelta. Sen sijaan termihakua käytettäessä hakutermit koskivat nimenomaan todentamisen ohittamista. Julkaisujen lisäksi myös haavoittuvuusluokattomien haavoittuvuuksien kohdalla käytettiin termihakua, eli termihaun kautta lisätyt haavoittuvuudet eivät myöskään ole koko väärän todennuksen alalta.

Tuloksista voidaan huomata tämä kategorioiden edustuksien ero julkaisujen ja haavoittuvuuksien välillä. Tästä voidaan päätellä, ettei kaikki väärän todennuksen alakategoriat olleet samallalailla edustettuina termihakua käytettäessä verraten hierarkkiseen hakuun, josta suurin osa haavoittuvuuksien kategorioiden edustuksesta löydettiin. Tällöin siis hierarkkisesti löydettyjä haavoittuvuuksia etsittiin suuremmalta skaalalta kuin termihaun avulla haettuja julkaisuja ja haavoittuvuuksia.

Julkaisujen kategorioiden ulkopuolella haavoittuvuuksia oli myös liittyen 12 muuhun alakategoriaan. Näitä olivat vajaasti suojellut tunnukset (CWE-522), kovakoodattujen tunnusten käyttö (CWE-798), sopimaton rajoitus liiallisille todentamisyrityksille (CWE-307), heikot salasanan vaatimukset (CWE-521), heikko unohdetun salasanan palautusmekanismi (CWE-640), heikko salasanan koodaus (CWE-261), todentamisen puute kriittisestä funktiosta (CWE-306), kriittisen vaiheen puute todentamisesta (CWE-304), sopimaton todentamisalgoritmin toteutus (CWE-303), varmistuksen puute salasananvaihdossa (CWE-620), todentamisen suorittaminen käyttäjäpuolella (CWE-603) sekä todentamisen ohittaminen ensisijaisen heikkouden avulla (CWE-305).

Yhdeksän väärän todennuksen alakategoriaa ei ollut edustettuina julkaisuissa eikä haavoittuvuuksissa: salasanan vanhenemisen puute (CWE-262) tai vanheneminen pitkällä erääntymi-

Kategoria	Julkaisut				Haavoittuvuudet			
	2019	2020	2021	Yhteensä	2019	2020	2021	Yhteensä
CWE-287	9	4	7	20	239	282	358	879
CWE-290	3	6	7	16	27	30	26	83
CWE-294	2	2	4	8	11	22	14	47
CWE-302	1	1	0	2	0	0	1	1
CWE-295	1	0	0	1	94	129	98	321
CWE-301	0	1	0	1	0	0	0	0
CWE-288	1	0	0	1	33	22	7	62
CWE-306	0	0	0	0	215	215	51	481
CWE-522	0	0	0	0	188	150	114	452
CWE-798	0	0	0	0	125	173	139	437
CWE-307	0	0	0	0	31	53	44	128
CWE-521	0	0	0	0	22	23	17	62
CWE-640	0	0	0	0	16	10	23	49
CWE-305	0	0	0	0	1	3	2	6
CWE-303	0	0	0	0	0	1	2	3
CWE-620	0	0	0	0	0	0	1	1
CWE-261	0	0	0	0	0	1	0	1
CWE-603	0	0	0	0	0	1	0	1
CWE-304	0	0	0	0	0	0	1	1
CWE-308	0	0	0	0	0	0	0	0
CWE-309	0	0	0	0	0	0	0	0
CWE-645	0	0	0	0	0	0	0	0
CWE-804	0	0	0	0	0	0	0	0
CWE-262	0	0	0	0	0	0	0	0
CWE-263	0	0	0	0	0	0	0	0
CWE-836	0	0	0	0	0	0	0	0
CWE-289	0	0	0	0	0	0	0	0
CWE-593	0	0	0	0	0	0	0	0

Taulukko 7. Julkaisut ja haavoittuvuudet kategorioittain vuosittain

#	2019	2020	2021	Kaikkiaan
1	CWE-287	CWE-290	CWE-287, CWE-290	CWE-287
2	CWE-290	CWE-287	CWE-294	CWE-290
3	CWE-294	CWE-294		CWE-294
4	CWE-302, CWE-295, CWE-288	CWE-302, CWE-301		CWE-302
5				CWE-295, CWE-301, CWE-288

Taulukko 8. Yleisimmät julkaisuissa esiintyneet kategoriat

sajalla (CWE-263), todentamisen ohittaminen käyttämällä vaihtoehtoista nimeä (CWE-289), yksivaiheisen todentamisen käyttäminen (CWE-308), salasanan käyttäminen pääasiallisena todentamisen tapana (CWE-309), todentamisen ohittaminen muuttamalla OpenSSL CTX-objektia SSL-objektien luonnin jälkeen (CWE-593), liikaa rajoittava käyttäjän lukitusmekanismi (CWE-645), arvattava CAPTCHA (CWE-804) sekä todentamisessa salasanatiivisteen käyttö salasanan sijaan (CWE-836).

Tulosten tarkemmaksi vertailemiseksi taulukoissa 8 ja 9 tuodaan esiin kategorioiden edustukset järjestettynä yleisyyden mukaan. Taulukosta 8 voidaan nähdä mitkä olivat yleisimmät kategoriat julkaisuissa tutkittavina vuosina. Vastaavasti taulukko 9 kuvastaa samaa haavoittuvuuksien kohdalla.

Sekä julkaisujen että haavoittuvuuksien kohdalla väärän todentamisen pääluokka on ensimmäisenä, paitsi julkaisuissa vuonna 2020 se on toisena. Julkaisuissa toiseksi yleisin kaikkiaan ja tutkittavina yksittäisinä vuosina ensimmäistä ja toista sijaa saanut todentamisen ohittaminen huijaamalla (CWE-290) on haavoittuvuuksissa vasta sijoilla 7–8. Julkaisuista kaikkiaan kolmantena, vuosittain sijoilla 2–3, on todentamisen ohittaminen toiston avulla (CWE-294).

Tämä on haavoittuvuuksissa sijoilla 9–11. Sijoittelua vertaillessa julkaisujen ja haavoittuvuuksien erot kategorioittain nousevat selkeästi esiin.

#	2019	2020	2021	Kaikkiaan
1	CWE-287	CWE-287	CWE-287	CWE-287
2	CWE-306	CWE-306	CWE-798	CWE-306
3	CWE-522	CWE-798	CWE-522	CWE-522
4	CWE-798	CWE-522	CWE-295	CWE-798
5	CWE-295	CWE-295	CWE-306	CWE-295
6	CWE-288	CWE-307	CWE-307	CWE-307
7	CWE-307	CWE-290	CWE-290	CWE-290
8	CWE-290	CWE-521	CWE-640	CWE-521, CWE-288
9	CWE-521	CWE-288, CWE-294	CWE-521	CWE-640
10	CWE-640	CWE-640	CWE-294	CWE-294
11	CWE-294	CWE-305	CWE-288	CWE-305
12	CWE-305	CWE-303, CWE-261, CWE-603	CWE-305, CWE-303	CWE-303
13			CWE-302, CWE-620, CWE-304	CWE-302, CWE-620, CWE-304, CWE-261, CWE-603

Taulukko 9. Yleisimmät haavoittuvuuksissa esiintyneet kategoriat

Vertailun helpottamiseksi taulukossa 10 haavoittuvuuksien kategoriat on rajoitettu ainoastaan niihin kategorioihin, joissa julkaisuista löytyi edustusta. Vertaamalla tätä taulukkoa yleisimpiin julkaisuihin (taulukko 8) huomataan, että julkaisujen kategorioihin nähden aiemmin

#	2019	2020	2021	Kaikkiaan
1	CWE-287	CWE-287	CWE-287	CWE-287
2	CWE-295	CWE-295	CWE-295	CWE-295
3	CWE-288	CWE-290	CWE-290	CWE-290
4	CWE-290	CWE-288, CWE-294	CWE-294	CWE-288
5	CWE-294		CWE-288	CWE-294
6			CWE-302	CWE-302

Taulukko 10. Yleisimmät haavoittuvuuksien kategoriat rajattuna julkaisuissa esiintyneisiin kategorioihin

mainittu todentamisen ohittaminen toiston avulla (CWE-294) on kaikkiaan toiseksi viimeisenä haavoittuvuuksissa. Sen sijaan kaikkiaan julkaisuissa jaetulle viimeiselle sijalle sijoittuva todentamisen ohittaminen käyttämällä vaihtoehtoista reittiä tai kanavaa (CWE-288) on haavoittuvuuksissa toiston kautta ohittamista yleisempää. Muuttumattomaksi oletetun datan (CWE-302) sijoitus vaihtoehtoisten reittien ja kanavien sijoitukseen nähden on jopa hyvin päinvastainen julkaisujen ja haavoittuvuuksien yleisyyksien välillä.

Julkaisuissa kaikkiaan eri vuosina sijoille 1–2 sijoittuva todentamisen ohittaminen huijaamalla (CWE-290) on haavoittuvuuksissa sijoilla 3–4, nostaen ylleen sopimattoman sertifikaatin validoinnin (CWE-295). Tämä taas kuuluu vähiten edustettuihin kategorioihin todentamisen ohittamiseen liittyvissä julkaisuissa.

Taulukossa 11 julkaisut ja haavoittuvuudet on vielä järjestetty sen perusteella, mikä todentamisen ohittamiseen nimensä mukaisesti liittyvä väärän todennuksen alakategoria on ollut yleisin kaikkien vuosien aikana. Molemmissa huijaamisen kautta tehty ohittaminen (CWE-290) on yleisin. Julkaisuissa toisena on ohittaminen toiston avulla (CWE-294), joka on haavoittuvuuksissa kolmantena. Haavoittuvuuksissa toisena on sen sijaan vaihtoehtoisen reitin tai kanavan käyttö (CWE-288), joka on julkaisuissa neljäntenä.

#	Julkaisut	Haavoittuvuudet
1	CWE-290	CWE-290
2	CWE-294	CWE-288
3	CWE-302	CWE-294
4	CWE-288	CWE-305
5	CWE-289, CWE-305, CWE-593	CWE-302
6		CWE-289, CWE-593

Taulukko 11. Yleisimmin esiintyvät todentamisen ohittamiseen nimensä mukaisesti liittyvät väärän todennuksen alakategoriat julkaisuissa ja haavoittuvuuksissa

Kolmantena julkaisuissa oli todentamisen ohittaminen muuttumattomaksi oletetun datan avulla (CWE-302). Tämä on haavoittuvuuksissa viidentenä heti ensisijaisen heikkouden kautta tapahtuvan ohittamisen (CWE-305) jälkeen. Tämä kategoria ei esiintynyt julkaisuissa lainkaan. Kummassakaan ei esiintynyt ohittamisen kategorioita vaihtoehtoisen nimen käyttämisestä (CWE-289) tai OpenSSL:n objektien muuttamiseen (CWE-593) liittyen.

9.4 Pohdinta

Löydetyissä julkaisuissa hylkäyssuhde oli korkea. Osittain tämä voi selittyä sillä, että hakutuloksista löytyi paljon julkaisuja, joihin ei ollut vapaata tai yliopiston lukuoikeuden alaista pääsyä. Siksi näitä ei voitu arvioida otettavaksi tutkimukseen mukaan. Julkaisuja olisi voinut yrittää myös luokitella pelkän metadatan perusteella, mutta tämä olisi voinut kuitenkin olla turhan haastavaa, koska luokittelu ei ollut yksinkertaista koko tekstin avullakaan. Poiketen alkuperäisestä ajatuksestani, julkaisuissa harvoin mainittiin CVE tai CWE -numeroita, jotka olisivat voineet auttaa kategorisoinnissa.

Lisäksi julkaisuissa esiintyi paljon tapauksia, joissa todentamisen ohittaminen mainittiin vain sivussa, eikä se ollut julkaisun tutkimuksen kohteena. Hylkäyssuhteen parantamiseksi tulisi miettiä miten hakua voitaisiin paremmin kohdistaa todentamisen ohittamista pääasiassa käsitteleviin julkaisuihin. Yksi vaihtoehto olisi, että julkaisuja olisi hyväksytty mukaan ke-

vyemmin ehdoin. Tällöin kuitenkin raja todentamisen ohittamista ja pelkkää todentamista käsittelevien julkaisujen välillä olisi häilyvämpi. Tässä tutkimuksessa pidettiin tärkeänä, että julkaisussa käsiteltiin nimenomaan todentamisen ohittamista tai sen estämistä selkeästi haavoittuvuuksien näkökulmasta. Julkaisu hylättiin, jos vahvemman todentamisen todettiin olevan tarpeellista ilman, että syitä tämän taustalla nostettiin selkeästi esiin. Tällöin pois lukeutui myös tapaukset, joissa todentamista parannetaan ainoastaan muista syistä, kuten esimerkiksi tehokkuuden tai resurssisyiden takia.

Hyvänä puolena hakutermeissä oli kuitenkin se, että hakujen avulla löytyi vain kaksi julkaisua, jotka eivät liittyneet tietotekniikkaan. Tässä suhteessa hakusanoilla saatiin hyvin rajattua pois samankaltaista terminologiaa käyttäviä muiden aiheiden tutkimuksia.

Jo ennen tutkimuksen aloittamista haavoittuvuuksien kohdalla huomattiin, että haavoittuvuusluokitusten käytössä voi esiintyä puutteita – joistakin haavoittuvuuksista puuttuu luokittelu. Termihaun avulla pyrittiin löytämään näistä lisää haavoittuvuuksia tutkimukseen, jotka hierarkkinen haku olisi jättänyt huomioimatta. Termihakua käytettiin kuitenkin vain haavoittuvuuksiin, joista puuttui haavoittuvuusluokitus kokonaan. Hakua olisi voinut laajentaa myös muissa kategorioissa esiintyviin haavoittuvuuksiin. Niistäkin olisi voinut löytyä todentamisen ohittamiseen liittyviä haavoittuvuuksia, joista vain puuttuu väärän todennuksen tai sen alakategorian luokitus.

Termihakujen kautta saaduista tuloksista huomattiin, etteivät ne edusta koko väärän todennuksen skaalaa, jonka alalta hierarkkista hakua tehtiin. Jos koko väärän todennuksen alaa haluttaisiin tutkia, tulisi termihakua miettiä senkin kannalta uudestaan.

Erityisesti termihaun haavoittuvuuksia kategorisoidessa huomasi, että haavoittuvuuksien kuvaukset voivat olla lyhyitä ja sisältää hyvin rajallisesti yksityiskohtia haavoittuvuuteen liittyen. Tämä on voinut olla myös syy siihen, miksi niille ei ole annettu haavoittuvuusluokitusta alunperinkään. Haavoittuvuuksissa esitetyn tiedon vähäisyyden voi arvella liittyvän esimerkiksi siihen, ettei haavoittuvuuksien yksityiskohtia haluta paljastaa, jotta niitä ei käytettäisi hyväksi hyökkäystarkoituksessa. Toisaalta tämä voi rajoittaa ymmärrystä siitä, kuinka vakavasta haavoittuvuudesta on kyse, voiden vaikuttaa suhtautumiseen kyseisen haavoittuvuuden korjaamiseksi.

Tämä tiedonpuute haavoittuvuuksien kuvauksissa voi myös kannustaa siihen, että haavoittuvuuksille annetaan korkeamman tason luokituksia tarkempien alaluokituksien sijaan. Sekä julkaisujen että haavoittuvuuksien kohdalla huomattiin, että pääluokka sai kaikista eniten edustusta. Tämän takia voidaan myös arvailla, että pääluokan suuri edustus voi liittyä siihen, ettei väärän todennuksen alla ole tarpeeksi kuvaavia alakategorioita. Tarvetta liian yksityiskohtaisille alakategorioille voidaan kuitenkin myös kyseenalaistaa, koska se voisi vähentää luokittelun merkitystä. Galhardo ja hänen kollegansa (2020, s. 163) huomasivat myös samankaltaisia ongelmia liittyen haavoittuvuuksien ja haavoittuvuusluokitusten kuvauksiin ja käyttöön.

Hierarkkisessa haavoittuvuuksien haussa haku tehtiin rajoittamalla hierarkian kulkeminen ylöspäin kolmeen polveen. Jälkikäteen polvien määrän lisäämistä testatessa tämä ei kuitenkaan näyttänyt vaikuttavan löytyneiden haavoittuvuuksien määrään. Lisäksi väärän todennuksen alaisia haavoittuvuusluokituksia selatessa voidaan huomata, että niiden alakategorioiden hierarkia päättyy kolmen polven aikana. Näiden puolesta voidaan todeta, että tutkimuksessa käytetty rajoitus oli riittävä.

10 Johtopäätökset

Kirjautumista vaativien järjestelmien ja niiden takana olevan tiedon määrä kasvaa vain vuosi vuodelta asioiden digitalisoituessa. Siksi on olennaista, että kaikki tämä tieto on mahdollisimman turvassa väärinkäytöltä. Tämän takia on tärkeää tarkastella minkä tyyppisiä ongelmia tulisi pitää mielessä järjestelmien kehitysprosessissa. Tässä tutkimuksessa pyrittiin antamaan kuvaa todentamisen ohittamisen tutkimuksen tämänhetkisestä tilanteesta. Tutkimuksen tilaa vuosina 2019–2021 verrattiin myös samana aikavälinä esiintyneisiin haavoittuvuuksiin.

Tutkimukseen hyväksyttiin mukaan 45 julkaisua. Julkaisujen ja haavoittuvuuksien vertailemiseksi haavoittuvuuksia löydettiin tutkitulta aikaväliltä yhteensä 3094. Tutkimuksen tuloksista nähdään, että todentamisen ohittamiseen liittyviä julkaisuja on julkaistu melko tasaisesti tutkittavien vuosien aikana. Julkaisut ovat pääasiassa kuvanneet ratkaisuja liittyen todentamisen ohittamiseen. Lisäksi hyökkäyksiä kuvaavia julkaisuja on lukuisia.

Julkaisuille tehtiin tutkimuksen aikana myös aiheittainen jako huomattujen yleisimpien aihealueiden perusteella. Aiheittain julkaisuja oli eniten liittyen laitteisiin ja yhteyksiin. Toiseksi eniten oli julkaisuja liittyen biometriseen todentamiseen. Näiden lisäksi julkaisuja oli myös liittyen muun muassa ohjelmoinnin kielellisiin ominaisuuksiin sekä monivaiheiseen todentamiseen.

Haavoittuvuusluokituksen pohjalta tehdystä kategorisoinnista huomattiin, että suurin osa julkaisuista käsittelee haavoittuvuuksia, jotka sopivat parhaiten suoraan väärän todennuksen pääluokkaan (CWE-287). Haavoittuvuustapauksien kategorisoinnissa huomattiin myös sama ilmiö. Tämä voi viitata esimerkiksi siihen, että väärän todennuksen alla ei ole tarpeeksi alakategorioita kuvaamaan tarkasti todentamisen ohittamisen eri muotoja.

Väärän todennuksen alakategorioissa julkaisuja oli eniten liittyen todentamisen ohittamiseen huijaamalla (CWE-290). Nämä julkaisut liittyivät usein biometriseen todentamiseen. Vuosittaisella tasolla voitiin huomata, että näitä julkaisuja on tullut vuosi vuodelta enemmän.

Toiseksi eniten julkaisuja oli todentamisen ohittamisesta toiston avulla (CWE-294). Julkaisuissa esiintyi myös vähemmällä edustuksella väärän todennuksen alakategoriat sopimatto-

masta sertifikaatin validoinnista (CWE-295), reflektiohyökkäyksen mahdollisuudesta todennusprotokollassa (CWE-301) sekä todentamisen ohittamisesta muuttumattomaksi oletetun datan avulla (CWE-302) tai käyttämällä vaihtoehtoista reittiä tai kanavaa (CWE-288).

Kategorisoinnissa huomattiin, todentamisen ohittamista käsittelevät julkaisut edustivat vain osaa väärän todentamisen alakategorioista. Haavoittuvuuksia ei myöskään löytynyt kaikista kategorioista tutkitulla aikavälillä, mutta ne edustivat silti huomattavasti isompaa joukkoa kuin julkaisujen kategoriat.

Nimensä mukaisesti todentamisen ohittamiseen liittyvistä alakategorioista todentamisen ohittaminen huijaamisen kautta (CWE-290) oli yleisin sekä julkaisuissa että haavoittuvuuksissa. Näin ollen tämä on ollut syystäkin tärkeänä tutkimuksen painotuksena. Todentamisen ohittaminen toiston avulla (CWE-294) esiintyy järjestyksen mukaan molemmissa melko samassa suhteessa, ollen sijoilla 2–3. Haavoittuvuuksissa toisiksi yleisimpänä oleva vaihtoehtoisen reitin tai kanavan käyttäminen (CWE-288) sen sijaan oli vasta neljäntenä julkaisuissa, mahdollisesti kaivaten tutkimuksessa lisähuomiota.

Loppuja näistä alakategorioista esiintyi vain vähän tai ei lainkaan sekä julkaisuissa että haavoittuvuuksissa. Nämä ovat todentamisen ohittaminen muuttumattomaksi oletetun datan avulla (CWE-302), ensisijaisen heikkouden avulla (CWE-305), käyttämällä vaihtoehtoista nimeä (CWE-289) ja muuttamalla OpenSSL CTX-objektia SSL-objektien luonnin jälkeen (CWE-593). Haavoittuvuuksien määrien perusteella nämä eivät ole tällä hetkellä yhtä relevantteja kategorioita kuin aiemmin mainitut todentamisen ohittamiseen liittyvät kategoriat.

Lähteet

Barker, Elaine, Dennis Branstad, Santosh Chokhani ja Miles Smid. 2010. *Cryptographic Key Management Workshop Summary - June 8-9, 2009.* https://doi.org/10.6028/NIST.IR.7609.

Cawthra, Jennifer, Sue Wang, Bronwyn Hodges, Kangmin Zheng, Ryan Williams, Jason Kuruvilla, Christopher Peloquin, Kevin Littlefield ja Bob Neimeyer. 2020. *Securing Picture Archiving and Communication System (PACS) Cybersecurity for the Healthcare Sector.* https://doi.org/10.6028/NIST.SP.1800-24.

Christey, Steve. 2007. "Unforgivable vulnerabilities". *Black Hat Briefings* 13:17.

Dalton, Michael, Christos Kozyrakis ja Nickolai Zeldovich. 2009. "Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Applications".

Finlex. 2009. *7.8.2009/617: Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.* https://www.finlex.fi/fi/laki/ajantasa/2009/20090617.

Frank, Mario, Ralf Biedert, Eugene Ma, Ivan Martinovic ja Dawn Song. 2012. "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication". *IEEE transactions on information forensics and security* 8 (1): 136–148.

Galhardo, Carlos Cardoso, Peter Mell, Irena Bojanova ja Assane Gueye. 2020. "Measurements of the most significant software security weaknesses". Teoksessa *Annual Computer Security Applications Conference,* 154–164.

Grance, Tim, Joan Hash, Steven Peck, Jonathan Smith ja Karen Korow-Diks. 2002. "NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems". *National Institute of Standards and Technology (NIST),* https://doi.org/10.6028/NIST.SP.800-47.

Grassi, Paul A, James L Fenton ja Michael E Garcia. 2017. "NIST Special Publication 800-63-3: Digital Identity Guidelines". *National Institute of Standards and Technology (NIST),* https://doi.org/10.6028/NIST.SP.800-63-3.

Grassi, Paul A, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richer, Naomi B Lefkovitz, Jamie M Danker, Yee-Yin Choong ym. 2017. "NIST Special Publication 800-63b: Digital Identity Guidelines: Authentication and Lifecycle Management". *National Institute of Standards and Technology (NIST),* https://doi.org/10.6028/NIST.SP.800-63b.

Kitchenham, Barbara, ja Stuart Charters. 2007. *Guidelines for performing systematic literature reviews in software engineering.* Technical report. EBSE.

Lalouani, Wassila, Mohamed Younis, Danila Frolov ja Uthman Baroudi. 2020. "Protocol Switching Mechanism for Countering Radiometric Signature Exploitation". Teoksessa *ICC 2020-2020 IEEE International Conference on Communications (ICC),* 1–7. IEEE.

MITRE. 2021a. *CAPEC-115: Authentication Bypass.* https://capec.mitre.org/data/definitions/115.html.

———. 2021b. *CAPEC-461: Web Services API Signature Forgery Leveraging Hash Function Extension Weakness.* https://capec.mitre.org/data/definitions/461.html.

———. 2021c. *CAPEC-480: Escaping Virtualization.* https://capec.mitre.org/data/definitions/480.html.

———. 2021d. *CAPEC-664: Server Side Request Forgery.* https://capec.mitre.org/data/definitions/664.html.

———. 2021e. *CAPEC-668: Key Negotiation of Bluetooth Attack (KNOB).* https://capec.mitre.org/data/definitions/668.html.

———. 2021f. *CAPEC-87: Forceful Browsing.* https://capec.mitre.org/data/definitions/87.html.

———. 2021g. *CWE Version 4.5.* https://cwe.mitre.org/data/published/cwe_v4.5.pdf.

NIST. 2021. *NVD - Home.* https://nvd.nist.gov/.

Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen ja Yevgeni Koucheryavy. 2018. “Multi-Factor Authentication: A Survey”. *Cryptography* 2 (1). ISSN: 2410-387X. https://doi.org/10.3390/cryptography2010001. https://www.mdpi.com/2410-387X/2/1/1.

OWASP. 2021a. *OWASP Top 10:2021: A07:2021 – Identification and Authentication Failures.* https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/.

———. 2021b. *WSTG - Latest: Testing for Bypassing Authentication Schema.* https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/04-Testing_for_Bypassing_Authentication_Schema.html.

Petersen, Kai, Robert Feldt, Shahid Mujtaba ja Michael Mattsson. 2008. “Systematic Mapping Studies in Software Engineering”. Teoksessa *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12,* 1–10.

Ren, Wei, Linchen Yu, Liangli Ma ja Yi Ren. 2013. “How to Authenticate a Device? Formal Authentication Models for M2M Communications Defending against Ghost Compromising Attack”. *International Journal of Distributed Sensor Networks* 9 (2): 679450. https://doi.org/10.1155/2013/679450. eprint: https://doi.org/10.1155/2013/679450. https://doi.org/10.1155/2013/679450.

Rui, Zhang, ja Zheng Yan. 2019. “A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification”. *IEEE Access* 7:5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996.

Shirey, R. 2007. *Internet Security Glossary, Version 2, RFC 4949.* RFC. https://www.rfc-editor.org/rfc/rfc4949.txt.

Shoshitaishvili, Yan, Ruoyu Wang, Christophe Hauser, Christopher Kruegel ja Giovanni Vigna. 2015. “Firmalice-Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware.” Teoksessa *NDSS,* 1:1–1.

Stouffer, Keith, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams ja Adam Hahn. 2015. “NIST Special Publication 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security”. *National Institute of Standards and Technology (NIST),* https://doi.org/10.6028/NIST.SP.800-82r2.

Wang, Enze, Baosheng Wang, Wei Xie, Zhenhua Wang, Zhenhao Luo ja Tai Yue. 2020. “EWVHunter: Grey-Box Fuzzing with Knowledge Guide on Embedded Web Front-Ends”. *Applied Sciences* 10 (11). ISSN: 2076-3417. https://doi.org/10.3390/app10114015. https://www.mdpi.com/2076-3417/10/11/4015.

Wiefling, Stephan, Luigi Lo Iacono ja Markus Dürmuth. 2019. “Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild”. Teoksessa *ICT Systems Security and Privacy Protection,* toimittanut Gurpreet Dhillon, Fredrik Karlsson, Karin Hedström ja André Zúquete, 134–148. Cham: Springer International Publishing. ISBN: 978-3-030-22312-0.

Wilhelm, Thomas, ja Jason Andress. 2011. “Chapter 16 - Sabotage”. Teoksessa *Ninja Hacking,* toimittanut Thomas Wilhelm ja Jason Andress, 267–284. Boston: Syngress. ISBN: 978-1-59749-588-2. https://doi.org/10.1016/B978-1-59749-588-2.00016-0.

Zviran, Moshe, ja Zippy Erlich. 2006. “Identification and authentication: technology and implementation issues”. *Communications of the Association for Information Systems* 17 (1): 4.

Liitteet

A Julkaisut

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
-	2021	Proceedings of the 30th USENIX Security Symposium	Scopus	kokoelma eikä yksittäinen julkaisu			
Ahn, Wonhyuk; Jang, Haneol; Nam, Seung-Hun; Yu, In-Jae; Lee, Heung-Kyu	2020	Local-Source Enhanced Residual Network for Steganalysis of Digital Images	IEEE	ei todentamisesta			
Aliero, M. S.; Qureshi, K. N.; Pasha, M. F.; Ahmad, A.; Jeon, G.	2020	Detection of structure query language injection vulnerability in web driven database application	Scopus		ratkaisu	CWE-287	kielet
Angelogianni, Anna; Politis, Ilias; Mohammadi, Farnaz; Xenakis, Christos	2020	On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats	IEEE	todentamiseen liittyvät ongelmat pienessä roolissa			
Arif Khan, F.; Kunhambu, S.; Chakravarthy G, K.	2019	Behavioral biometrics and machine learning to secure website logins	Scopus	todentamisen jälkeen sen ylläpitäminen			
Aski, V.; Dhaka, V. S.; Parashar, A.	2021	An Attribute-Based Break-Glass Access Control Framework for Medical Emergencies	Scopus	ei saatavilla			
Awang, N. F.; Manaf, A. A.; Jarno, A. D.	2019	Automated test input generation for detecting SQL injection vulnerability using set theory concept	Scopus		ratkaisu	CWE-287	kielet
Awang, Nor Fatimah; Jarno, Ahmad Dahari; Marzuki, Syahaneim; Jamaludin, Nor Azliana Akmal; Majid, Khairani Abd; Tajuddin, Taniza	2019	Method For Generating Test Data For Detecting SQL Injection Vulnerability in Web Application	IEEE, Scopus		ratkaisu	CWE-287	kielet

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Ba, Zhongjie; Zhang, Xinyu; Qin, Zhan; Ren, Kui	2019	CFP: Enabling Camera Fingerprint Concealment for Privacy-Preserving Image Sharing	IEEE, Scopus		ratkaisu	CWE-290	laitteet ja yhteydet
Benamara, Nadir Kamel; Keche, Mokhtar; Wellington, Murisi; Munyaradzi, Zhou	2021	Securing E-payment Systems by RFID and Deep Facial Biometry	IEEE, Scopus	todentamisen ohittaminen mainitaan vain lyhyesti			
Benegui, C.; Ionescu, R. T.	2021	Improving the authentication with built-in camera protocol using built-in motion sensors: A deep learning solution	Scopus		ratkaisu	CWE-290	laitteet ja yhteydet
Benzidane, K.; Khoudali, S.; Fetjah, L.; Andaloussi, S. J.; Sekkaki, A.	2019	Application-based authentication on an inter-VM traffic in a cloud environment	Scopus	mainitaan todentamisen lisäämisestä			
Bhalla, R.; Jeyanthi, N.	2020	M2U2: Multifactor mobile based unique user authentication mechanism	Scopus	ei saatavilla			
Bhuyan, R.; Kenny, S. P. K.; Borah, S.; Mishra, D.; Das, K.	2021	Recent Advancements in Continuous Authentication Techniques for Mobile-Touchscreen-Based Devices	Scopus	ei saatavilla			
Bisht, P.; Rauthan, M. S.; Bisht, R. K.	2019	Component based web application firewall for analyzing and defending SQL injection attack vectors	Scopus		ratkaisu	CWE-287	kielet
Bore, J.	2020	Insider threat	Scopus	ei saatavilla			
Brinkmann, M.; Dresen, C.; Merget, R.; Poddebniak, D.; Müller, J.; Somorovsky, J.; Schwenk, J.; Schinzel, S.	2021	ALPACA: Application layer protocol confusion - Analyzing and mitigating cracks in TLS authentication	Scopus	ei saatavilla			
Buchade, A.; Ingle, R.; Potdar, V.	2021	Elastic Security for Autonomic Computing Using Intelligent Algorithm	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Bui, T.; Rao, S.; Antikainen, M.; Aura, T.	2019	Client-side vulnerabilities in commercial VPNs	Scopus		ratkaisu	CWE-294, CWE-295	laitteet ja yhteydet
Burkert, Christian; McDougall, Johanna Ansohn; Federrath, Hannes; Fischer, Mathias	2021	Analysing Leakage during VPN Establishment in Public Wi-Fi Networks	IEEE, Scopus	ei todentamisen ohittamisesta			
Büttner, A.; Nguyen, H. V.; Gruschka, N.; Lo Iacono, L.	2021	Less is Often More: Header Whitelisting as Semantic Gap Mitigation in HTTP-Based Software Systems	Scopus	ei saatavilla			
Campobasso, M.; Allodi, L.	2020	Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale	Scopus		pohdinta	CWE-290	MFA
Chandrasekara, P.; Abeywardana, H.; Rajapaksha, S.; Parameshwaran, S.; Yapa Abeywardana, K.	2020	Behavior and Biometrics Based Masquerade Detection Mobile Application	Scopus	ei saatavilla			
Charles, Subodha; Mishra, Prabhat	2020	Lightweight and Trust-Aware Routing in NoC-Based SoCs	IEEE, Scopus	ei todentamisen ohittamisesta, mietitään tunnistustehokkuutta			
Chaudhary, S.; Nath, R.; Kant, C.; Kant, S.	2019	Approach for protection of iris template using cancelable biometrics	Scopus	ei saatavilla			
Chen, J.; Paxson, V.; Jiang, J.	2020	Composition kills: A case study of email sender authentication	Scopus	ei saatavilla			
Chi, Kuang-Hui; Kustiawan, Iwan	2020	Handover-Supporting Streamlined Networking	IEEE	ei todentamisen ohittamisesta			
Chinchole, Rutwik; Kakad, Aditya; Bhirud, Sumit; Raghunath, Aakarsh; Mumbaikar, Ms. Snehal	2019	Online CAPTCHA Replacement through Face Detection	IEEE, Scopus	vain lyhyesti CAPTCHA:n heikkouksista			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Chowdhary, Ankur; Sabur, Abdulhakim; Huang, Dijiang; Kirby, James; Kang, M.	2021	Object Oriented Policy Conflict Checking Framework in Cloud Networks (OOPC)	IEEE, Scopus	todentamisen ohittamistapaus taustasyynä ratkaisun kehittämiselle			
Cui, Q.; Zhao, W.; Gu, X.; Zhu, Z.; Zhu, X.; Tao, X.; Ni, W.	2021	Efficient handover authentication and secure key-updating mechanism for B5G networks	Scopus	ei saatavilla			
Das, T. R.; Hasan, S.; Sarwar, S. M.; Das, J. K.; Rahman, M. A.	2021	Facial spoof detection using support vector machine	Scopus	ei saatavilla			
Davaslioglu, Kemal; Sagduyu, Yalin E.	2019	Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning	IEEE, Scopus		ratkaisu	CWE-287	laitteet ja yhteydet
De Pessemier, T.; Coppens, I.; Martens, L.	2020	Evaluating facial recognition services as interaction technique for recommender systems	Scopus	ohitetaan palautteen antaminen			
Du, P.; Nakao, A.; Miki, S.; Inoue, M.	2020	Design and implementation of 10 Gbps software PPPoE router for Iot smart home network	Scopus	ei saatavilla			
Dunphy, P.; Vlachokyriakos, V.; Thieme, A.; Nicholson, J.; McCarthy, J.; Olivier, P.	2019	Social media as a resource for understanding security experiences: A qualitative analysis of #password tweets	Scopus	ei saatavilla			
Ellahi, O.; Shah, M. A.; Rana, M. U.	2021	The ingenuity of malware substitution: Bypassing next-generation Antivirus	Scopus	ei todentamisesta			
Elliot, Kwesi; Graham, Jonathan; Yassin, Yusef; Ward, Trenton; Caldwell, John; Attie, Tawab	2019	A Comparison of Machine Learning Algorithms in Keystroke Dynamics	IEEE, Scopus	todentamistapa, ei ohittamisesta			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Engelbertz, N.; Mladenov, V.; Somorovsky, J.; Herring, D.; Erinola, N.; Schwenk, J.	2019	Security analysis of XADES validation in the CEF digital signature Services (DSS)	Scopus	ei saatavilla			
Etienne, Laeticia; Shahriar, Hossain	2020	Attacks and Mitigation Techniques for Iris-Based Authentication Systems	IEEE, Scopus		hyökkäys	CWE-290	biometria
Fan, Y.; Liu, J.; Li, K.-C.; liang , W.; Lei, X.; Tan, G.; Tang, M.	2021	One enhanced secure access scheme for outsourced data	Scopus	todentamisen ohittaminen mainitaan vaan tiivistelmässä			
Farkhani, R. M.; Ahmadi, M.; Lu, L.	2021	PTAuth: Temporal memory safety via robust points-to authentication	Scopus	ei saatavilla			
Fern, N.; Cheng, K.-T. T.	2019	Pre-silicon Formal Verification of JTAG Instruction Opcodes for Security	Scopus	mainitaan todentamisen mahdollisesta lisäämisestä			
Ferreira, Anselmo; Chen, Changsheng; Barni, Mauro	2021	Fusing Multiscale Texture and Residual Descriptors for Multilevel 2D Barcode Rebroadcasting Detection	IEEE		ratkaisu	CWE-290	muu
Fiterau-Bro?tean, P.; Jonsson, B.; Merget, R.; de Ruiter, J.; Sagonas, K.; Somorovsky, J.	2020	Analysis of DTLS implementations using protocol state fuzzing	Scopus	ei saatavilla			
Ford, Kerry; De Cusatis, Casimer; Otis, Michael	2021	Bypassing Fingerprint Scanners Using Artifical Fingerprints	IEEE		hyökkäys	CWE-290	biometria
Franken, Gertjan; Van Goethem, Tom; Joosen, Wouter	2019	Exposing Cookie Policy Flaws Through an Extensive Evaluation of Browsers and Their Extensions	IEEE	evästeiden ongelmista, ei todentamisen ohittamisesta			
Ganesh, A.; Safa, M.; Roopanjali, M.; Sai Sri Harsha, P. V. K.; Anjana Tulasi, D.	2020	An approach for monitoring and analyzing parking occupancies using IoT	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Gilkalaye, Babak Poorebrahim; Derakhshani, Reza	2021	Biometrically Trusted Personal Health Status for Pandemic Management	IEEE	ei todentamisen ohittamisesta			
Gkougkas, E.; Arizabaleta, M.; Pany, T.; Eissfeller, B.	2019	A novel authentication signal component for codeless correlation	Scopus	ei saatavilla			
Goldschmidt, Patrik; Ku?era, Jan	2021	Defense Against SYN Flood DoS Attacks Using Network-based Mitigation Techniques	IEEE, Scopus	ei todentamisen ohittamisesta			
Griffioen, Paul; Weerakkody, Sean; Sinopoli, Bruno	2021	A Moving Target Defense for Securing Cyber-Physical Systems	IEEE, Scopus	ei todentamisen ohittamisesta			
Grimes, R.	2019	The many ways to hack 2FA	Scopus	ei saatavilla			
Hoang, X. D.	2021	Detecting Common Web Attacks Based on Machine Learning Using Web Log	Scopus	ei saatavilla			
Hoang, X. D.; Nguyen, T. H.	2021	Detecting common web attacks based on supervised machine learning using web logs	Scopus	ei saatavilla			
Hoque, T.; Yang, K.; Karam, R.; Tajik, S.; Forte, D.; Tehranipoor, M.; Bhunia, S.	2019	Hidden in plaintext: An obfuscation-based countermeasure against FPGA bitstream tampering attacks	Scopus		ratkaisu	CWE-287	laitteet ja yhteydet
Hyndavi, K.; Siva Nageswara Rao, G.	2020	A logical analysis perspective of Ios devices	Scopus	ei saatavilla			
Irshad, A.; Chaudhry, S. A.; Shafiq, M.; Usman, M.; Asif, M.; Ghani, A.	2019	A provable and secure mobile user authentication scheme for mobile cloud computing services	Scopus		ratkaisu	CWE-290, CWE-294	muu
Jeong, E.; Park, J.; Oh, I.; Kim, M.; Yim, K.	2021	Analysis on account hijacking and remote dos vulnerability in the codesys-based plc runtime	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Jubur, M.; Shrestha, P.; Saxena, N.; Prakash, J.	2021	Bypassing Push-based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications	Scopus	käyttäjä hyväksyy vahingossa hyökkääjän todentamisen, ei varsinaisesti ohita			
Kallepalli, K.; Chaudhry, U. B.	2021	Intelligent Security: Applying Artificial Intelligence to Detect Advanced Cyber Attacks	Scopus	ei saatavilla			
Kaur, D.; Kumar, D.	2021	Cryptanalysis and improvement of a two-factor user authentication scheme for smart home	Scopus		ratkaisu	CWE-294	laitteet ja yhteydet
Kim, E.; Choi, H.-K.	2021	Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild	Scopus		hyökkäys	CWE-290	MFA
Kim, Hongil; Lee, Jiho; Lee, Eunkyu; Kim, Yongdae	2019	Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane	IEEE		hyökkäys	CWE-287	laitteet ja yhteydet
Lalouani, W.; Younis, M.; Baroudi, U.	2021	Countering radiometric signature exploitation using adversarial machine learning based protocol switching	Scopus	estetään laitekohtaisen sormenjäljen syntymistä jotta sitä ei voida hyödyntää todentamisessa			
Lalouani, Wassila; Younis, Mohamed; Frolov, Danila; Baroudi, Uthman	2020	Protocol Switching Mechanism for Countering Radiometric Signature Exploitation	IEEE, Scopus	laitekohtaisen sormenjäljen syntyminen			
Lee, K.; Kaiser, B.; Mayer, J.; Narayanan, A.	2020	An empirical study of wireless carrier authentication for SIM swaps	Scopus	ei saatavilla			
Lee, K.; Oh, I.; Jang, W.; Choi, C.; Yim, K.	2019	Vulnerability Analysis on a Secure USB: Based on a Commercial Product A	Scopus	ei saatavilla			
Lee, W. Q. J.; Ong, T. S.; Connie, T.; Jackson, H. T.	2021	Finger Vein Presentation Attack Detection with Optimized LBP Variants	Scopus		ratkaisu	CWE-290	biometria

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Leguesse, Yonas; Colombo, Christian; Vella, Mark; Hernandez-Castro, Julio	2021	PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone	IEEE, Scopus		ratkaisu	CWE-294	MFA
Li, Chi-Yu; Lin, Ying-Dar; Lai, Yuan-Cheng; Chien, Hsu-Tung; Huang, Yu-Sheng; Huang, Po-Hao; Liu, Hsueh-Yang	2020	Transparent AAA Security Design for Low-Latency MEC-Integrated Cellular Networks	IEEE, Scopus	ei todentamisen ohittamisesta			
Li, H.; Pan, X.; Wang, X.; Feng, H.; Shi, C.	2020	Authenticator Rebinding Attack of the UAF Protocol on Mobile Devices	Scopus		hyökkäys	CWE-294	MFA
Li, P.; Meng, W.	2021	LChecker: Detecting loose comparison bugs in PHP	Scopus		ratkaisu	CWE-287	kielet
Li, Q.; Chen, H.	2019	CDAs: A continuous dynamic authentication system	Scopus	todentamisen jälkeen sen ylläpitäminen			
Li, Z.; Wang, J.; Zhang, W.	2020	Revisiting post-quantum hash proof systems over lattices for Internet of Thing authentications	Scopus	kvanttiresistenssi, ei ohittamisesta			
Li, Zengpeng; Wang, Ding; Morais, Eduardo	2020	Quantum-Safe Round-Optimal Password Authentication for Mobile Devices	IEEE, Scopus	kvanttiresisti todentaminen, ei ohittamisesta			
Limniotis, K.	2021	Cryptography as the means to protect fundamental human rights	Scopus	kryptografiasta, ei todentamisen ohittamisesta			
Liu, Y.; Squires, M. R.; Taylor, C. R.; Walls, R. J.; Shue, C. A.	2019	Account Lockouts: Characterizing and Preventing Account Denial-of-Service Attacks	Scopus	ei saatavilla			
Longari, S.; Penco, M.; Carminati, M.; Zanero, S.	2019	CopyCAN: An error-handling protocol based intrusion detection system for controller area network	Scopus	todentaminen ei käytössä			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Ma, Q.; Wang, W.; Guan, T.; Liu, Y.; Lin, L.	2020	Modbus Protocol Based on the Characteristics of the Transmission of Industrial Data Packet Forgery Tampering and Industrial Security Products Testing	Scopus	ei saatavilla			
Marcus Tan, Yi Xiang; Iacovazzi, Alfonso; Homoliak, Ivan; Elovici, Yuval; Binder, Alexander	2019	Adversarial Attacks on Remote User Authentication Using Behavioural Mouse Dynamics	IEEE, Scopus		hyökkäys	CWE-287	biometria
Marrone, S.; Sansone, C.	2021	On the transferability of adversarial perturbation attacks against fingerprint based authentication systems	Scopus		hyökkäys	CWE-290	biometria
Marrone, Stefano; Sansone, Carlo	2019	Adversarial Perturbations Against Fingerprint Based Authentication Systems	IEEE, Scopus		hyökkäys	CWE-290	biometria
Meharaj Begum, A.; Arock, Michael	2021	Efficient Detection Of SQL Injection Attack(SQLIA) Using Pattern-based Neural Network Model	IEEE, Scopus		ratkaisu	CWE-287	kielet
Mehta, Nandish; Tell, Stephen; Turner, Walker; Tatro, Lamar; Goh, Giant; Gray, C. Thomas	2021	A 77 MHz Relaxation Oscillator in 5nm FinFET with 3ns TIE over 10K cycles and ±0.3% Thermal Stability using Frequency-Error Feedback Loop	IEEE		ratkaisu	CWE-287	laitteet ja yhteydet
Mirian, A.; DeBlasio, J.; Savage, S.; Voelker, G. M.; Thomas, K.	2019	Hack for Hire: Exploring the emerging market for account hijacking	Scopus	tietojen kalastelua, ei ohittamista			
Mladenov, V.; Mainka, C.; Zu Selhausen, K. M.; Grothe, M.; Schwenk, J.	2019	1 trillion dollar refund - How to spoof PDF signatures	Scopus	sertifikaatin validointiongelma, ei todentamisen ohittamisesta			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Monjirul Kabir, M.; Hasan, N.; Khalid Hassan Tahmid, M. D.; Ovi, T. A.; Rozario, V. S.	2020	Enhancing smartphone lock security using vibration enabled randomly positioned numbers	Scopus	PIN-koodin arvaamisesta, ei ohittamisesta			
Narayanankutty, H.; Srinivasan, C.	2020	Novel Authentication System for Personal and Domestic Network Systems Using Image Feature Comparison and Digital Signatures	Scopus	ei saatavilla			
Nirmal, K.; Janet, B.; Kumar, R.	2019	Enhancing online security using selective DOM approach to counter phishing attacks	Scopus	ei saatavilla			
Nursiah, N.; Wong, K.; Kuribayashi, M.	2019	Reversible data hiding in PDF document exploiting prefix zeros in glyph coordinates	Scopus	ei todentamisesta			
Oh, J.; Choi, J.; Moon, K.; Lee, K.	2021	Research on Implementation of User Authentication Based on Gesture Recognition of Human	Scopus	ei saatavilla			
Ojewale, M. A.; Yomsi, P. M.	2019	Multi-factor authentication and fingerprint-based debit card system	Scopus	todentamisen ohittaminen mainitaan vaan lyhyesti syyksi lisätä monivaiheista todennusta			
Park, J.; Park, Y.	2020	Symmetric-key cryptographic routine detection in anti-reverse engineered binaries using hardware tracing	Scopus	ei todentamisesta			
Parmar, Abhishek; Gada, Sagar; Loke, Trunesh; Jain, Yash; Pathak, Sujata; Patil, Sonali	2021	Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP	IEEE	äänestämisessä todentamisen kehittäminen, ei ohittamisesta			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Pasquale, Liliana; Zippo, Paola; Curley, Cliona; O'Neill, Brian; Mongiello, Marina	2020	Digital Age of Consent and Age Verification: Can They Protect Children?	IEEE, Scopus	todentamisen lisääminen sovellusten ikärajoituksiin			
Patel, Chintan; Doshi, Nishant	2019	Cryptanalysis of ecc-based key agreement scheme for generic IoT network model	IEEE, Scopus	yhdyskäytävän ohitus, ei todentamisen			
Penchalaiah, P.; Vijay Kumar, M.; Ramesh Reddy, K.	2019	A research threshold efficient hybrid encryption schema for secure file system	Scopus	lähtökohtana että todennus ei ole esteenä			
Phun, Josephine Angeline Poetri Yanes; Safitri, Cutifa	2021	Smartphone Authentication with Hand Gesture Recognition (HGR) Using LiDAR	IEEE	todentamistapa, ei ohittamisesta			
Praseetha, V. M.; Bayezeed, S.; Vadivel, S.	2020	Secure fingerprint authentication using deep learning and minutiae verification	Scopus		ratkaisu	CWE-290	biometria
Priyadarshini, I.; Cotton, C.	2020	Internet Memes: A Novel Approach to Distinguish Humans and Bots for Authentication	Scopus	ei saatavilla			
Priyadarshini, I.; Wang, H.; Cotton, C.	2020	Some Cyberpsychology Techniques to Distinguish Humans and Bots for Authentication	Scopus	ei saatavilla			
Qiu, P.; Wang, D.; Lyu, Y.; Qu, G.	2019	Voltjockey: Breaching trustzone by software-controlled voltage manipulation over multi-core frequencies	Scopus		hyökkäys	CWE-302	laitteet ja yhteydet
Ramesh, Mridhula; Akruthi, S.; Nandhini, K.; Meena, S.; Joseph Gladwin, S.; Rajavel, R.	2019	Implementation of Vehicle Security System using GPS,GSM and Biometric	IEEE, Scopus	todentamisen ohittamisen käsittely rajoittuu siihen mitä tehdään jos se on tapahtunut			
Rohini; Sharma, K.	2019	Chain based routing algorithm using hybrid optimisation for wireless sensor network	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Sahoo, Subham; Yang, Yongheng; Blaabjerg, Frede	2021	Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks	IEEE	ei todentamisen ohittamisesta			
Sani, A. S.; Yuan, D.; Bertino, E.; Dong, Z. Y.	2021	Crypto-Chain: A Relay Resilience Framework for Smart Vehicles	Scopus		ratkaisu	CWE-294	MFA
Sani, Abubakar Sadiq; Yuan, Dong; Meng, Ke; Dong, Zhao Yang	2021	R-Chain: A Universally Composable Relay Resilience Framework for Smart Grids	IEEE		ratkaisu	CWE-294	laitteet ja yhteydet
Schepers, D.; Ranganathan, A.; Vanhoef, M.	2019	Practical side-channel attacks against WPA-TKIP	Scopus		hyökkäys	CWE-288	laitteet ja yhteydet
Shen, K.; Wang, C.; Guo, M.; Zheng, X.; Lu, C.; Liu, B.; Zhao, Y.; Hao, S.; Duan, H.; Pan, Q.; Yang, M.	2021	Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks	Scopus	ei saatavilla			
Shi, Yi; Davaslioglu, Kemal; Sagduyu, Yalin E.	2021	Generative Adversarial Network in the Air: Deep Adversarial Learning for Wireless Signal Spoofing	IEEE, Scopus		hyökkäys	CWE-290	laitteet ja yhteydet
Shibuya, Y.; Mwitondi, K.; Zargari, S.	2020	Experimental analyses in search of effective mitigation for login cross-site request forgery	Scopus	ei saatavilla			
Singh, Shivshakti; Inamdar, Aditi; Kore, Aishwarya; Pawar, Aprupa	2020	Analysis of Algorithms for User Authentication using Keystroke Dynamics	IEEE, Scopus	todentamistapa, ei ohittamisesta kuin maininta liittyen muihin tapoihin			
Skorobogatov, Sergei	2020	Compromising device security via NVM controller vulnerability	IEEE, Scopus		hyökkäys	CWE-290, CWE-302	laitteet ja yhteydet
Srivastava, V.; Debnath, S. K.	2021	Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme	Scopus		hyökkäys	CWE-287	muu
Stobert, E.; Safaie, T.; Molyneaux, H.; Mannan, M.; Youssef, A.	2020	ByPass: Reconsidering the usability of password managers	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Sulaiman, N.; Tajul Ariffin, Q. A.	2020	Overview on Fingerprinting Authentication Technology	Scopus	ei saatavilla			
Sunardi; Riadi, I.; Raharja, P. A.	2019	Vulnerability analysis of E-voting application using open web application security project (OWASP) framework	Scopus	OWASP avulla haavoittuvuuksien löytäminen järjestelmästä			
Talukdar, Jonti; Chen, Siyuan; Das, Amitabh; Aftabjahani, Sohrab; Song, Peilin; Chakrabarty, Krishnendu	2021	A BIST-based Dynamic Obfuscation Scheme for Resilience against Removal and Oracle-guided Attacks	IEEE, Scopus		ratkaisu	CWE-287	laitteet ja yhteydet
Talwar, M.; Balusamy, B.	2020	Iot secured disjunctive xor two factor mutual authentication for users	Scopus	ei saatavilla			
Tang, Z.; Feng, X.; Xie, Y.; Phan, H.; Guo, T.; Yuan, B.; Wei, S.	2020	VVSec: Securing Volumetric Video Streaming via Benign Use of Adversarial Perturbation	Scopus		ratkaisu	CWE-290	biometria
Taranov, K.; Rothenberger, B.; Perrig, A.; Hoefler, T.	2020	sRDMA - Efficient NIC-based authentication and encryption for remote direct memory access	Scopus	ei saatavilla			
Touhiduzzaman, Md; Hahn, Adam; Srivastava, Anurag K.	2019	A Diversity-Based Substation Cyber Defense Strategy Utilizing Coloring Games	IEEE		hyökkäys	CWE-287	laitteet ja yhteydet
Vadlamudi, Gnana Abhinay; Kishan, Kondaveeti Hari	2021	Security Authentication using Brain Waves	IEEE, Scopus	todentamistapa, ohittamista pohditaan alussa muihin tapoihin liittyen			
Vanhoef, Mathy; Ronen, Eyal	2020	Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd	IEEE, Scopus		hyökkäys	CWE-287, CWE-301	laitteet ja yhteydet
Voris, J.; Song, Y.; Salem, M. B.; Hershkop, S.; Stolfo, S.	2019	Active authentication using file system decoys and user behavior modeling: results of a large scale study	Scopus	todentamisen jälkeen sen ylläpitäminen			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Wang, E.; Wang, B.; Xie, W.; Wang, Z.; Luo, Z.; Yue, T.	2020	EWVHunter: Grey-box fuzzing with knowledge guide on embedded web front-ends	Scopus		ratkaisu	CWE-287	kielet
Wang, Fei; Li, Zhenjiang; Han, Jinsong	2019	Continuous User Authentication by Contactless Wireless Sensing	IEEE, Scopus	todentamistapa, ei ohittamisesta			
Wang, J.; Hu, F.; Zhou, Y.; Liu, Y.; Zhang, H.; Liu, Z.	2020	BlueDoor: Breaking the secure information flow via BLE vulnerability	Scopus		hyökkäys	CWE-294	laitteet ja yhteydet
Warimani, M.; Azami, M. H.; Savill, M.; Li, Y.-G.; Khan, S. A.; Ismail, A. F.	2019	Investigation of aircraft engine performance utilizing various alternative fuels	Scopus	ei liity tietotekniikkaan			
Weisbord, R. K.; Horton, D.	2020	Inheritance Forgery	Scopus	ei saatavilla			
Wilder, Vabrice T.; Gao, Yujing; Wang, Shuangbao Paul; Perez, Alfredo J.	2019	Multi-Factor Stateful Authentication using NFC, and Mobile Phones	IEEE, Scopus	todentamistapa, ei ohittamisesta			
Xie, Tian; Tu, Guan-Hua; Yin, Bangjie; Li, Chi-Yu; Peng, Chunyi; Zhang, Mi; Liu, Hui; Liu, Xiaoming	2021	The Untold Secrets of WiFi-Calling Services: Vulnerabilities, Attacks, and Countermeasures	IEEE	ei todentamisen haavoittuvuuksista			
Xu, Dongyang; Yu, Keping; Ritcey, James A.	2021	Cross-Layer Device Authentication with Quantum Encryption for 5G Enabled IIoT in Industry 4.0	IEEE	todentamisen lisääminen sen oltua pois käytöstä resurssisyistä			
Xu, F.; Shen, S.; DIao, W.; Li, Z.; Chen, Y.; Li, R.; Zhang, K.	2021	Android on PC: On the Security of End-user Android Emulators	Scopus	todentaminen puuttuu			
Xu, Qizhen; Zhang, Zhijie; Zhang, Lin; Chen, Liwei; Shi, Gang	2021	Finding Runtime Usable Gadgets: On the Security of Return Address Authentication	IEEE		hyökkäys	CWE-287	muu

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Xu, Y.-W.; Wang, R.; Zhang, C.-M.	2021	Discrete-phase-randomized twin-field quantum key distribution without phase postselection in the test mode	Scopus	ei todentamisen ohittamisesta			
Yin, X.; Liu, S.; Jia, F.; Xiao, D.	2020	REDT: Remote exploitation detection technology for network infrastructure	Scopus		ratkaisu	CWE-287	laitteet ja yhteydet
Yu, Y.-C.; Chen, Z.-N.; Gan, S.-T.; Qin, X.-J.	2021	Research on the Technologies of Security Analysis Technologies on the Embedded Device Firmware	Scopus	ei saatavilla kokonaan englanniksi			
Zaidi, A. Z.; Chong, C. Y.; Jin, Z.; Parthiban, R.; Sadiq, A. S.	2021	Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities	Scopus	todentamisen jälkeen sen ylläpitäminen			
Zelmer, C.; Zweifel, L. P.; Kapinos, L. E.; Craciun, I.; Güven, Z. P.; Palivan, C. G.; Lim, R. Y. H.	2020	Organelle-specific targeting of polymersomes into the cell nucleus	Scopus	ei liity tietotekniikkaan			
Zhang, L.; Chen, J.; Diao, W.; Guo, S.; Weng, J.; Zhang, K.	2019	CRYPTOREX: Large-scale analysis of cryptographic misuse in IoT devices	Scopus	ei saatavilla			
Zhang, Long; Zhang, Donghong; Wang, Chenghong; Zhao, Jing; Zhang, Zhenyu	2019	ART4SQLi: The ART of SQL Injection Vulnerability Discovery	IEEE, Scopus		ratkaisu	CWE-287	kielet
Zhang, Tianchen; Zhang, Taimin; Ji, Xiaoyu; Xu, Wenyuan	2019	Cuckoo-RPL: Cuckoo Filter based RPL for Defending AMI Network from Blackhole Attacks	IEEE, Scopus	todentaminen puuttuu			
Zhang, X.; Gu, D.; Zhang, C.	2020	Issues of identity verification of typical applications over mobile terminal platform	Scopus	ei saatavilla			

Tekijät	Vuosi	Nimi	Lähde	Hylkäyssyy	Tyyppi	Kategoria	Aihe
Zhu, Tiantian; Fu, Lei; Liu, Qiang; Lin, Zi; Chen, Yan; Chen, Tieming	2021	One Cycle Attack: Fool Sensor-Based Personal Gait Authentication With Clustering	IEEE, Scopus		ratkaisu	CWE-287	biometria
Zolotarev, Vyacheslav V.; Knyazuk, Semen O.; Maro, Ekaterina A.	2020	Liveness Detection Mechanisms to Enhance Robustness of Authentication Methods in Game-Based Educational Services	IEEE, Scopus		ratkaisu	CWE-290	biometria
Zoppi, T.; Schiavone, E.; Bicchierai, I.; Brancati, F.; Bondavalli, A.	2021	Spoofing detectability as a property of biometric characteristics	Scopus	ei saatavilla			

B Manuaalisesti luokitellut haavoittuvuudet

CWE	Määrä	CVE:t
CWE-288	3	CVE-2019-9939, CVE-2020-13297, CVE-2019-19964
CWE-290	1	CVE-2019-9733
CWE-294	1	CVE-2020-1676
CWE-307	2	CVE-2020-4128, CVE-2020-4129
CWE-798	1	CVE-2019-9733
CWE-287	46	CVE-2021-31924, CVE-2020-0943, CVE-2020-11445, CVE-2020-11788, CVE-2020-11989, CVE-2020-15506, CVE-2020-1957, CVE-2020-26926, CVE-2020-4493, CVE-2020-4499, CVE-2019-10256, CVE-2019-19873, CVE-2019-19878, CVE-2019-20642, CVE-2019-20681, CVE-2019-20690, CVE-2019-20760, CVE-2019-4210, CVE-2019-4241, CVE-2019-5347, CVE-2019-5396, CVE-2019-7964, CVE-2019-8081, CVE-2020-13933, CVE-2020-23355, CVE-2019-0101, CVE-2019-0173, CVE-2019-11210, CVE-2019-12428, CVE-2019-13531, CVE-2019-13953, CVE-2019-15067, CVE-2019-15069, CVE-2019-15088, CVE-2019-18225, CVE-2019-19556, CVE-2019-20490, CVE-2019-20492, CVE-2019-20498, CVE-2019-3629, CVE-2019-3706, CVE-2019-3707, CVE-2019-3717, CVE-2019-3910, CVE-2019-5134, CVE-2019-9196
Hylätyt	35	CVE-2021-1302, CVE-2021-1304, CVE-2021-1534, CVE-2021-36235, CVE-2020-13952, CVE-2020-1748, CVE-2020-24513, CVE-2020-26927, CVE-2020-26928, CVE-2020-29189, CVE-2020-3444, CVE-2020-4461, CVE-2020-4485, CVE-2020-4611, CVE-2020-5580, CVE-2020-5582, CVE-2020-5583, CVE-2020-5632, CVE-2020-8602, CVE-2019-0057, CVE-2019-1044, CVE-2019-1593, CVE-2019-1730, CVE-2019-18181, CVE-2019-19774, CVE-2019-19980, CVE-2019-5933, CVE-2019-5935, CVE-2019-5941, CVE-2019-5942, CVE-2019-5943, CVE-2019-5944, CVE-2019-6023, CVE-2019-6614, CVE-2020-1241

C Väärän todentamisen haavoittuvuudet

CWE	Vuosi	Määrä	CVE:t
CWE-288	2019	33	CVE-2019-11326, CVE-2019-1220, CVE-2019-12583, CVE-2019-12768, CVE-2019-13030, CVE-2019-13981, CVE-2019-14347, CVE-2019-14927, CVE-2019-16340, CVE-2019-16386, CVE-2019-16388, CVE-2019-17503, CVE-2019-17643, CVE-2019-17644, CVE-2019-17645, CVE-2019-17646, CVE-2019-1898, CVE-2019-1899, CVE-2019-20484, CVE-2019-2388, CVE-2019-25012, CVE-2019-3916, CVE-2019-3917, CVE-2019-3933, CVE-2019-3934, CVE-2019-6126, CVE-2019-6551, CVE-2019-7736, CVE-2019-9552, CVE-2019-9584, CVE-2019-9884, CVE-2019-9939, CVE-2019-19964
	2020	22	CVE-2020-10181, CVE-2020-10248, CVE-2020-11561, CVE-2020-13474, CVE-2020-13850, CVE-2020-15633, CVE-2020-17409, CVE-2020-24660, CVE-2020-24765, CVE-2020-26150, CVE-2020-27863, CVE-2020-27865, CVE-2020-27866, CVE-2020-28937, CVE-2020-29656, CVE-2020-35391, CVE-2020-35570, CVE-2020-4050, CVE-2020-7541, CVE-2020-8116, CVE-2020-8439, CVE-2020-13297
	2021	7	CVE-2021-24046, CVE-2021-27453, CVE-2021-33017, CVE-2021-36308, CVE-2021-41292, CVE-2021-43935, CVE-2021-43985

CWE-290	2019	27	CVE-2019-0283, CVE-2019-0388, CVE-2019-0608, CVE-2019-10875, CVE-2019-11189, CVE-2019-12131, CVE-2019-1234, CVE-2019-1318, CVE-2019-1357, CVE-2019-13701, CVE-2019-13703, CVE-2019-13704, CVE-2019-13708, CVE-2019-13709, CVE-2019-13715, CVE-2019-15022, CVE-2019-16378, CVE-2019-16871, CVE-2019-18259, CVE-2019-18659, CVE-2019-18989, CVE-2019-18990, CVE-2019-18991, CVE-2019-20203, CVE-2019-20790, CVE-2019-25023, CVE-2019-9733
	2020	30	CVE-2020-10135, CVE-2020-10136, CVE-2020-10807, CVE-2020-11015, CVE-2020-11091, CVE-2020-12272, CVE-2020-1329, CVE-2020-1331, CVE-2020-13529, CVE-2020-16250, CVE-2020-17516, CVE-2020-2002, CVE-2020-2033, CVE-2020-24375, CVE-2020-26254, CVE-2020-26276, CVE-2020-27276, CVE-2020-27847, CVE-2020-27970, CVE-2020-28856, CVE-2020-36128, CVE-2020-4290, CVE-2020-4421, CVE-2020-4864, CVE-2020-5415, CVE-2020-6808, CVE-2020-6810, CVE-2020-7326, CVE-2020-7327, CVE-2020-7388
	2021	26	CVE-2021-1677, CVE-2021-20278, CVE-2021-21134, CVE-2021-21215, CVE-2021-21216, CVE-2021-21310, CVE-2021-21492, CVE-2021-22779, CVE-2021-22890, CVE-2021-23984, CVE-2021-28372, CVE-2021-28810, CVE-2021-29441, CVE-2021-30619, CVE-2021-30621, CVE-2021-32076, CVE-2021-32631, CVE-2021-34561, CVE-2021-34646, CVE-2021-36942, CVE-2021-41130, CVE-2021-42308, CVE-2021-42320, CVE-2021-43220, CVE-2021-43807, CVE-2021-43890
CWE-294	2019	11	CVE-2019-11334, CVE-2019-11856, CVE-2019-12393, CVE-2019-12887, CVE-2019-13533, CVE-2019-18226, CVE-2019-20626, CVE-2019-3915, CVE-2019-5307, CVE-2019-9158, CVE-2019-9659
	2020	22	CVE-2020-10045, CVE-2020-10185, CVE-2020-12355, CVE-2020-12692, CVE-2020-13799, CVE-2020-14302, CVE-2020-15688, CVE-2020-23178, CVE-2020-24722, CVE-2020-25229, CVE-2020-25660, CVE-2020-26172, CVE-2020-27157, CVE-2020-27269, CVE-2020-28713, CVE-2020-35551, CVE-2020-4042, CVE-2020-5261, CVE-2020-5300, CVE-2020-6972, CVE-2020-9438, CVE-2020-1676
	2021	14	CVE-2021-22267, CVE-2021-25480, CVE-2021-25834, CVE-2021-25835, CVE-2021-26824, CVE-2021-27195, CVE-2021-27572, CVE-2021-27662, CVE-2021-35067, CVE-2021-38459, CVE-2021-40170, CVE-2021-41025, CVE-2021-41030, CVE-2021-46145
CWE-295	2019	94	CVE-2019-0054, CVE-2019-1003009, CVE-2019-1006, CVE-2019-10091, CVE-2019-1010206, CVE-2019-1010275, CVE-2019-10314, CVE-2019-10317, CVE-2019-10334, CVE-2019-10381, CVE-2019-10382, CVE-2019-10444, CVE-2019-10446, CVE-2019-10914, CVE-2019-11242, CVE-2019-11324, CVE-2019-11497, CVE-2019-11550, CVE-2019-11554, CVE-2019-11674, CVE-2019-11688, CVE-2019-11727, CVE-2019-12000, CVE-2019-1231, CVE-2019-12496, CVE-2019-12855, CVE-2019-13050, CVE-2019-14334, CVE-2019-14516, CVE-2019-14823, CVE-2019-14910, CVE-2019-15042, CVE-2019-1552, CVE-2019-15525, CVE-2019-15604, CVE-2019-1590, CVE-2019-16179, CVE-2019-16209, CVE-2019-16252, CVE-2019-16263, CVE-2019-16281, CVE-2019-16558, CVE-2019-16561, CVE-2019-1659, CVE-2019-1683, CVE-2019-17007, CVE-2019-1748, CVE-2019-17560, CVE-2019-1757, CVE-2019-1859, CVE-2019-18632, CVE-2019-18633, CVE-2019-18826, CVE-2019-18847, CVE-2019-1886, CVE-2019-19101, CVE-2019-19270, CVE-2019-19271, CVE-2019-1940, CVE-2019-1948, CVE-2019-20455, CVE-2019-20894, CVE-2019-3685, CVE-2019-3751, CVE-2019-3762, CVE-2019-3777, CVE-2019-3807, CVE-2019-3814, CVE-2019-3841, CVE-2019-3875, CVE-2019-3890, CVE-2019-4150, CVE-2019-4264, CVE-2019-4654, CVE-2019-5101, CVE-2019-5102, CVE-2019-5280, CVE-2019-5506, CVE-2019-5537, CVE-2019-5538, CVE-2019-5729, CVE-2019-5961, CVE-2019-6032, CVE-2019-6266, CVE-2019-6592, CVE-2019-6687, CVE-2019-6702, CVE-2019-7615, CVE-2019-7728, CVE-2019-8337, CVE-2019-8351, CVE-2019-8531, CVE-2019-8642, CVE-2019-9148
	2020	129	CVE-2020-0119, CVE-2020-0601, CVE-2020-10059, CVE-2020-10659, CVE-2020-10925, CVE-2020-11050, CVE-2020-1113, CVE-2020-11176, CVE-2020-11580, CVE-2020-11617, CVE-2020-11792, CVE-2020-11806, CVE-2020-12143, CVE-2020-12144, CVE-2020-12421, CVE-2020-12637, CVE-2020-12681, CVE-2020-13163, CVE-2020-13245, CVE-2020-13254, CVE-2020-13482, CVE-2020-13614, CVE-2020-13615, CVE-2020-13616, CVE-2020-13645, CVE-2020-13955, CVE-2020-14039, CVE-2020-14387, CVE-2020-14980, CVE-2020-14981, CVE-2020-15047, CVE-2020-15133, CVE-2020-15134, CVE-2020-15260, CVE-2020-15498, CVE-2020-15526, CVE-2020-15604, CVE-2020-15719, CVE-2020-15720, CVE-2020-15732, CVE-2020-15813, CVE-2020-16162, CVE-2020-16163, CVE-2020-16164, CVE-2020-16197, CVE-2020-16228, CVE-2020-1675, CVE-2020-17366, CVE-2020-1758, CVE-2020-1887, CVE-2020-1929, CVE-2020-1952, CVE-2020-2033, CVE-2020-2187, CVE-2020-2252, CVE-2020-2253, CVE-2020-24025, CVE-2020-24392, CVE-2020-24393, CVE-2020-24560, CVE-2020-24613, CVE-2020-24619, CVE-2020-24661, CVE-2020-24714, CVE-2020-24715, CVE-2020-25276, CVE-2020-25680, CVE-2020-26117, CVE-2020-27589, CVE-2020-27648, CVE-2020-27649, CVE-2020-28362, CVE-2020-28907, CVE-2020-28942, CVE-2020-28972, CVE-2020-29440, CVE-2020-29457, CVE-2020-29663, CVE-2020-3155, CVE-2020-3342, CVE-2020-3557, CVE-2020-35662, CVE-2020-35733, CVE-2020-36127, CVE-2020-36425, CVE-2020-36477, CVE-2020-36478, CVE-2020-3940, CVE-2020-3994, CVE-2020-4320, CVE-2020-4340, CVE-2020-4496, CVE-2020-4791, CVE-2020-5367, CVE-2020-5520, CVE-2020-5521, CVE-2020-5522, CVE-2020-5523, CVE-2020-5526, CVE-2020-5684, CVE-2020-5812, CVE-2020-5864, CVE-2020-5909, CVE-2020-5913, CVE-2020-6175, CVE-2020-6529, CVE-2020-6781, CVE-2020-7041, CVE-2020-7042, CVE-2020-7043, CVE-2020-7904, CVE-2020-7919, CVE-2020-7922, CVE-2020-7924, CVE-2020-7942, CVE-2020-7956, CVE-2020-8156, CVE-2020-8172, CVE-2020-8279, CVE-2020-8286, CVE-2020-8289, CVE-2020-8987, CVE-2020-9040, CVE-2020-9321, CVE-2020-9432, CVE-2020-9433, CVE-2020-9434, CVE-2020-9488, CVE-2020-9868

	2021	98	CVE-2021-0341, CVE-2021-1134, CVE-2021-1276, CVE-2021-1277, CVE-2021-1354, CVE-2021-1471, CVE-2021-1566, CVE-2021-1837, CVE-2021-20109, CVE-2021-20110, CVE-2021-20230, CVE-2021-20327, CVE-2021-20328, CVE-2021-20435, CVE-2021-20649, CVE-2021-20732, CVE-2021-20833, CVE-2021-21373, CVE-2021-21374, CVE-2021-21385, CVE-2021-21559, CVE-2021-21571, CVE-2021-22138, CVE-2021-22189, CVE-2021-22218, CVE-2021-22278, CVE-2021-22511, CVE-2021-22895, CVE-2021-22909, CVE-2021-22926, CVE-2021-22939, CVE-2021-23155, CVE-2021-23162, CVE-2021-23167, CVE-2021-24012, CVE-2021-25633, CVE-2021-25634, CVE-2021-26320, CVE-2021-26911, CVE-2021-27018, CVE-2021-27098, CVE-2021-27189, CVE-2021-27257, CVE-2021-27400, CVE-2021-27899, CVE-2021-28363, CVE-2021-29495, CVE-2021-29504, CVE-2021-29653, CVE-2021-29737, CVE-2021-31399, CVE-2021-31597, CVE-2021-31747, CVE-2021-31892, CVE-2021-32069, CVE-2021-32574, CVE-2021-32581, CVE-2021-32727, CVE-2021-32728, CVE-2021-32755, CVE-2021-3285, CVE-2021-32919, CVE-2021-3309, CVE-2021-3336, CVE-2021-33695, CVE-2021-33907, CVE-2021-3450, CVE-2021-34558, CVE-2021-34599, CVE-2021-3460, CVE-2021-35193, CVE-2021-35497, CVE-2021-3636, CVE-2021-36371, CVE-2021-36377, CVE-2021-36382, CVE-2021-36756, CVE-2021-37218, CVE-2021-37219, CVE-2021-37698, CVE-2021-38864, CVE-2021-39358, CVE-2021-39359, CVE-2021-39360, CVE-2021-39361, CVE-2021-39365, CVE-2021-40713, CVE-2021-40828, CVE-2021-40829, CVE-2021-40830, CVE-2021-40831, CVE-2021-40855, CVE-2021-41019, CVE-2021-41028, CVE-2021-41611, CVE-2021-42027, CVE-2021-44273, CVE-2021-44549
CWE-305	2019	1	CVE-2019-14833
	2020	3	CVE-2020-10923, CVE-2020-14359, CVE-2020-15787
	2021	2	CVE-2021-21403, CVE-2021-3850
CWE-306	2019	215	CVE-2019-0246, CVE-2019-0261, CVE-2019-0312, CVE-2019-0379, CVE-2019-10039, CVE-2019-10040, CVE-2019-10041, CVE-2019-10042, CVE-2019-10046, CVE-2019-1010136, CVE-2019-10119, CVE-2019-10121, CVE-2019-10198, CVE-2019-10668, CVE-2019-10886, CVE-2019-10915, CVE-2019-10919, CVE-2019-10941, CVE-2019-10946, CVE-2019-10950, CVE-2019-11019, CVE-2019-11020, CVE-2019-11061, CVE-2019-11063, CVE-2019-11321, CVE-2019-11466, CVE-2019-11496, CVE-2019-11523, CVE-2019-11684, CVE-2019-12105, CVE-2019-12114, CVE-2019-12115, CVE-2019-12116, CVE-2019-12117, CVE-2019-12118, CVE-2019-12119, CVE-2019-12120, CVE-2019-12125, CVE-2019-12126, CVE-2019-12127, CVE-2019-12128, CVE-2019-12129, CVE-2019-12130, CVE-2019-12174, CVE-2019-12288, CVE-2019-12289, CVE-2019-12389, CVE-2019-12390, CVE-2019-12392, CVE-2019-12468, CVE-2019-12500, CVE-2019-12503, CVE-2019-12505, CVE-2019-12506, CVE-2019-12524, CVE-2019-12634, CVE-2019-12890, CVE-2019-12919, CVE-2019-13101, CVE-2019-13131, CVE-2019-13194, CVE-2019-13205, CVE-2019-13338, CVE-2019-13344, CVE-2019-13405, CVE-2019-13406, CVE-2019-13523, CVE-2019-13525, CVE-2019-13547, CVE-2019-13549, CVE-2019-13933, CVE-2019-13983, CVE-2019-14253, CVE-2019-14511, CVE-2019-14927, CVE-2019-14984, CVE-2019-15018, CVE-2019-15043, CVE-2019-15064, CVE-2019-15068, CVE-2019-15102, CVE-2019-15106, CVE-2019-15129, CVE-2019-15282, CVE-2019-15506, CVE-2019-15511, CVE-2019-15654, CVE-2019-15655, CVE-2019-15819, CVE-2019-15858, CVE-2019-15895, CVE-2019-15896, CVE-2019-15932, CVE-2019-15940, CVE-2019-16003, CVE-2019-16004, CVE-2019-16199, CVE-2019-16243, CVE-2019-16258, CVE-2019-16271, CVE-2019-1629, CVE-2019-1631, CVE-2019-1654, CVE-2019-16731, CVE-2019-16879, CVE-2019-16893, CVE-2019-16906, CVE-2019-16907, CVE-2019-17146, CVE-2019-17186, CVE-2019-17219, CVE-2019-17232, CVE-2019-17234, CVE-2019-17235, CVE-2019-17353, CVE-2019-17354, CVE-2019-17505, CVE-2019-17506, CVE-2019-17511, CVE-2019-17512, CVE-2019-17532, CVE-2019-18230, CVE-2019-18284, CVE-2019-18311, CVE-2019-18339, CVE-2019-18465, CVE-2019-18666, CVE-2019-1876, CVE-2019-18925, CVE-2019-18937, CVE-2019-18938, CVE-2019-18939, CVE-2019-1895, CVE-2019-1897, CVE-2019-18980, CVE-2019-19092, CVE-2019-19104, CVE-2019-19142, CVE-2019-19143, CVE-2019-19224, CVE-2019-19225, CVE-2019-19226, CVE-2019-19799, CVE-2019-19800, CVE-2019-19822, CVE-2019-20105, CVE-2019-20143, CVE-2019-20529, CVE-2019-20532, CVE-2019-20550, CVE-2019-20559, CVE-2019-20579, CVE-2019-20595, CVE-2019-20598, CVE-2019-20624, CVE-2019-25020, CVE-2019-3411, CVE-2019-3899, CVE-2019-3941, CVE-2019-3948, CVE-2019-3978, CVE-2019-4244, CVE-2019-4337, CVE-2019-4551, CVE-2019-5014, CVE-2019-5077, CVE-2019-5078, CVE-2019-5080, CVE-2019-5152, CVE-2019-5164, CVE-2019-5451, CVE-2019-5504, CVE-2019-5514, CVE-2019-5591, CVE-2019-5617, CVE-2019-5620, CVE-2019-5643, CVE-2019-5644, CVE-2019-6447, CVE-2019-6451, CVE-2019-6533, CVE-2019-6538, CVE-2019-6542, CVE-2019-6543, CVE-2019-6652, CVE-2019-6808, CVE-2019-6820, CVE-2019-6958, CVE-2019-7389, CVE-2019-7390, CVE-2019-7404, CVE-2019-7564, CVE-2019-7642, CVE-2019-7727, CVE-2019-8292, CVE-2019-8449, CVE-2019-8522, CVE-2019-8682, CVE-2019-8985, CVE-2019-8993, CVE-2019-9082, CVE-2019-9105, CVE-2019-9125, CVE-2019-9201, CVE-2019-9484, CVE-2019-9529, CVE-2019-9585, CVE-2019-9727, CVE-2019-9871, CVE-2019-9879, CVE-2019-9880, CVE-2019-9881, CVE-2019-9934, CVE-2019-9935, CVE-2019-9974

	2020	215	CVE-2020-0052, CVE-2020-10038, CVE-2020-10044, CVE-2020-10079, CVE-2020-10263, CVE-2020-10264, CVE-2020-10265, CVE-2020-10272, CVE-2020-10282, CVE-2020-10291, CVE-2020-10537, CVE-2020-10605, CVE-2020-10625, CVE-2020-10641, CVE-2020-10754, CVE-2020-10833, CVE-2020-10874, CVE-2020-10920, CVE-2020-10921, CVE-2020-10965, CVE-2020-10972, CVE-2020-10973, CVE-2020-10974, CVE-2020-11028, CVE-2020-11539, CVE-2020-11579, CVE-2020-11598, CVE-2020-11599, CVE-2020-11649, CVE-2020-11651, CVE-2020-11673, CVE-2020-11856, CVE-2020-11961, CVE-2020-11969, CVE-2020-12004, CVE-2020-12017, CVE-2020-12106, CVE-2020-12117, CVE-2020-12127, CVE-2020-12266, CVE-2020-12478, CVE-2020-12500, CVE-2020-12505, CVE-2020-12506, CVE-2020-12621, CVE-2020-12720, CVE-2020-12877, CVE-2020-13150, CVE-2020-13289, CVE-2020-13382, CVE-2020-13405, CVE-2020-13695, CVE-2020-13837, CVE-2020-13838, CVE-2020-13856, CVE-2020-13920, CVE-2020-14048, CVE-2020-14245, CVE-2020-14501, CVE-2020-15127, CVE-2020-15136, CVE-2020-15243, CVE-2020-15335, CVE-2020-15336, CVE-2020-15391, CVE-2020-15483, CVE-2020-15798, CVE-2020-15799, CVE-2020-15834, CVE-2020-15851, CVE-2020-15894, CVE-2020-16098, CVE-2020-16102, CVE-2020-16167, CVE-2020-17475, CVE-2020-1813, CVE-2020-1955, CVE-2020-19670, CVE-2020-20472, CVE-2020-20627, CVE-2020-2076, CVE-2020-21936, CVE-2020-23448, CVE-2020-23512, CVE-2020-24051, CVE-2020-24217, CVE-2020-24363, CVE-2020-24580, CVE-2020-24588, CVE-2020-25048, CVE-2020-25228, CVE-2020-25563, CVE-2020-25621, CVE-2020-25697, CVE-2020-25747, CVE-2020-25824, CVE-2020-25966, CVE-2020-26061, CVE-2020-26173, CVE-2020-26192, CVE-2020-26567, CVE-2020-26599, CVE-2020-26649, CVE-2020-26821, CVE-2020-26822, CVE-2020-26823, CVE-2020-26824, CVE-2020-26829, CVE-2020-26876, CVE-2020-27019, CVE-2020-27225, CVE-2020-27285, CVE-2020-27902, CVE-2020-27985, CVE-2020-27986, CVE-2020-28899, CVE-2020-28929, CVE-2020-28937, CVE-2020-28946, CVE-2020-29058, CVE-2020-29138, CVE-2020-29165, CVE-2020-29311, CVE-2020-29379, CVE-2020-29389, CVE-2020-29551, CVE-2020-3142, CVE-2020-3333, CVE-2020-3376, CVE-2020-3392, CVE-2020-3402, CVE-2020-3448, CVE-2020-3461, CVE-2020-35184, CVE-2020-35185, CVE-2020-35186, CVE-2020-35187, CVE-2020-35189, CVE-2020-35190, CVE-2020-35191, CVE-2020-35192, CVE-2020-35193, CVE-2020-35195, CVE-2020-35196, CVE-2020-35197, CVE-2020-35226, CVE-2020-3531, CVE-2020-35462, CVE-2020-35463, CVE-2020-35464, CVE-2020-35465, CVE-2020-35466, CVE-2020-35467, CVE-2020-35468, CVE-2020-35469, CVE-2020-35951, CVE-2020-3598, CVE-2020-36245, CVE-2020-36333, CVE-2020-3920, CVE-2020-3977, CVE-2020-4471, CVE-2020-4958, CVE-2020-5022, CVE-2020-5326, CVE-2020-5328, CVE-2020-5373, CVE-2020-5589, CVE-2020-5780, CVE-2020-5870, CVE-2020-5910, CVE-2020-6170, CVE-2020-6186, CVE-2020-6198, CVE-2020-6207, CVE-2020-6235, CVE-2020-6242, CVE-2020-6263, CVE-2020-6287, CVE-2020-6294, CVE-2020-6309, CVE-2020-6769, CVE-2020-6875, CVE-2020-6964, CVE-2020-7048, CVE-2020-7114, CVE-2020-7115, CVE-2020-7128, CVE-2020-7369, CVE-2020-7370, CVE-2020-7389, CVE-2020-7479, CVE-2020-7540, CVE-2020-7589, CVE-2020-7953, CVE-2020-7954, CVE-2020-7964, CVE-2020-8497, CVE-2020-8509, CVE-2020-8598, CVE-2020-8636, CVE-2020-9004, CVE-2020-9062, CVE-2020-9143, CVE-2020-9208, CVE-2020-9275, CVE-2020-9278, CVE-2020-9315, CVE-2020-9325, CVE-2020-9330, CVE-2020-9349, CVE-2020-9473, CVE-2020-9480, CVE-2020-9487, CVE-2020-9544
	2021	51	CVE-2021-1011, CVE-2021-1393, CVE-2021-1396, CVE-2021-1499, CVE-2021-20152, CVE-2021-20198, CVE-2021-20262, CVE-2021-20474, CVE-2021-20662, CVE-2021-20697, CVE-2021-20998, CVE-2021-21535, CVE-2021-22279, CVE-2021-22316, CVE-2021-22322, CVE-2021-22652, CVE-2021-22772, CVE-2021-22784, CVE-2021-22995, CVE-2021-23843, CVE-2021-23847, CVE-2021-25312, CVE-2021-26705, CVE-2021-26928, CVE-2021-27255, CVE-2021-27395, CVE-2021-28809, CVE-2021-28913, CVE-2021-29442, CVE-2021-31337, CVE-2021-31868, CVE-2021-32659, CVE-2021-32700, CVE-2021-32709, CVE-2021-32800, CVE-2021-32930, CVE-2021-33221, CVE-2021-33543, CVE-2021-33882, CVE-2021-34870, CVE-2021-37843, CVE-2021-38147, CVE-2021-3825, CVE-2021-38540, CVE-2021-39879, CVE-2021-41104, CVE-2021-41266, CVE-2021-42539, CVE-2021-42783, CVE-2021-43832, CVE-2021-45232
CWE-307	2019	31	CVE-2019-0039, CVE-2019-1126, CVE-2019-12941, CVE-2019-13166, CVE-2019-14299, CVE-2019-14351, CVE-2019-14951, CVE-2019-15577, CVE-2019-16670, CVE-2019-17215, CVE-2019-17240, CVE-2019-17525, CVE-2019-18235, CVE-2019-18261, CVE-2019-18917, CVE-2019-18985, CVE-2019-18986, CVE-2019-20031, CVE-2019-20881, CVE-2019-3746, CVE-2019-3766, CVE-2019-4068, CVE-2019-4310, CVE-2019-4336, CVE-2019-4393, CVE-2019-4520, CVE-2019-5217, CVE-2019-5263, CVE-2019-5309, CVE-2019-5421, CVE-2019-6524
	2020	53	CVE-2020-10849, CVE-2020-10876, CVE-2020-11052, CVE-2020-11650, CVE-2020-12645, CVE-2020-12752, CVE-2020-13312, CVE-2020-13617, CVE-2020-13805, CVE-2020-13835, CVE-2020-13872, CVE-2020-14484, CVE-2020-14494, CVE-2020-15367, CVE-2020-15770, CVE-2020-15786, CVE-2020-15906, CVE-2020-1616, CVE-2020-18698, CVE-2020-21237, CVE-2020-21238, CVE-2020-23283, CVE-2020-24007, CVE-2020-25196, CVE-2020-25827, CVE-2020-26556, CVE-2020-27423, CVE-2020-27747, CVE-2020-28206, CVE-2020-28212, CVE-2020-29042, CVE-2020-29136, CVE-2020-35565, CVE-2020-35585, CVE-2020-35586, CVE-2020-35590, CVE-2020-4193, CVE-2020-4232, CVE-2020-4400, CVE-2020-4567, CVE-2020-4891, CVE-2020-5141, CVE-2020-6852, CVE-2020-7057, CVE-2020-7508, CVE-2020-7525, CVE-2020-7995, CVE-2020-8202, CVE-2020-8228, CVE-2020-8790, CVE-2020-8827, CVE-2020-4128, CVE-2020-4129
	2021	44	CVE-2021-1311, CVE-2021-20427, CVE-2021-20635, CVE-2021-22003, CVE-2021-22915, CVE-2021-25676, CVE-2021-27188, CVE-2021-27514, CVE-2021-27935, CVE-2021-27943, CVE-2021-28127, CVE-2021-28248, CVE-2021-28909, CVE-2021-28911, CVE-2021-29023, CVE-2021-29648, CVE-2021-29842, CVE-2021-29987, CVE-2021-3138, CVE-2021-31646, CVE-2021-32522, CVE-2021-32678, CVE-2021-32703, CVE-2021-32705, CVE-2021-33190, CVE-2021-33209, CVE-2021-3412, CVE-2021-35472, CVE-2021-36284, CVE-2021-36285, CVE-2021-3663, CVE-2021-36750, CVE-2021-37934, CVE-2021-38155, CVE-2021-38474, CVE-2021-38725, CVE-2021-38890, CVE-2021-41171, CVE-2021-41435, CVE-2021-41807, CVE-2021-42096, CVE-2021-42544, CVE-2021-43332, CVE-2021-44033
CWE-521	2019	22	CVE-2019-13918, CVE-2019-17444, CVE-2019-18828, CVE-2019-18872, CVE-2019-18988, CVE-2019-19093, CVE-2019-19690, CVE-2019-19747, CVE-2019-3758, CVE-2019-4067, CVE-2019-4235, CVE-2019-4321, CVE-2019-4565, CVE-2019-4576, CVE-2019-4698, CVE-2019-6558, CVE-2019-7488, CVE-2019-7674, CVE-2019-7676, CVE-2019-9096, CVE-2019-9123, CVE-2019-9950
	2020	23	CVE-2020-11624, CVE-2020-11966, CVE-2020-15115, CVE-2020-15369, CVE-2020-25153, CVE-2020-26103, CVE-2020-26201, CVE-2020-27585, CVE-2020-27587, CVE-2020-29591, CVE-2020-4245, CVE-2020-4574, CVE-2020-6991, CVE-2020-6995, CVE-2020-7492, CVE-2020-7519, CVE-2020-7940, CVE-2020-8296, CVE-2020-8632, CVE-2020-8790, CVE-2020-8956, CVE-2020-8988, CVE-2020-9023

	2021	17	CVE-2021-1522, CVE-2021-20418, CVE-2021-20470, CVE-2021-25839, CVE-2021-25923, CVE-2021-26797, CVE-2021-28912, CVE-2021-28914, CVE-2021-32753, CVE-2021-35498, CVE-2021-38462, CVE-2021-39064, CVE-2021-40333, CVE-2021-41296, CVE-2021-41696, CVE-2021-43036, CVE-2021-43471
CWE-522	2019	188	CVE-2019-0032, CVE-2019-0035, CVE-2019-0072, CVE-2019-0120, CVE-2019-0175, CVE-2019-0178, CVE-2019-0179, CVE-2019-0180, CVE-2019-0182, CVE-2019-0183, CVE-2019-0881, CVE-2019-1000001, CVE-2019-1003038, CVE-2019-1003039, CVE-2019-1003045, CVE-2019-1003096, CVE-2019-1003097, CVE-2019-1010241, CVE-2019-1010308, CVE-2019-10139, CVE-2019-1020009, CVE-2019-10205, CVE-2019-10206, CVE-2019-10210, CVE-2019-10214, CVE-2019-10225, CVE-2019-10239, CVE-2019-10277, CVE-2019-10280, CVE-2019-10281, CVE-2019-10282, CVE-2019-10283, CVE-2019-10284, CVE-2019-10285, CVE-2019-10286, CVE-2019-10287, CVE-2019-10288, CVE-2019-10291, CVE-2019-10294, CVE-2019-10295, CVE-2019-10296, CVE-2019-10297, CVE-2019-10298, CVE-2019-10299, CVE-2019-10302, CVE-2019-10303, CVE-2019-10313, CVE-2019-10316, CVE-2019-10318, CVE-2019-10329, CVE-2019-10345, CVE-2019-10347, CVE-2019-10361, CVE-2019-10366, CVE-2019-10378, CVE-2019-10379, CVE-2019-10385, CVE-2019-10398, CVE-2019-10433, CVE-2019-10448, CVE-2019-10459, CVE-2019-10460, CVE-2019-10461, CVE-2019-10467, CVE-2019-10476, CVE-2019-10630, CVE-2019-10705, CVE-2019-10706, CVE-2019-10921, CVE-2019-10960, CVE-2019-10981, CVE-2019-11092, CVE-2019-11271, CVE-2019-11272, CVE-2019-11284, CVE-2019-11350, CVE-2019-11367, CVE-2019-11369, CVE-2019-11402, CVE-2019-11663, CVE-2019-11664, CVE-2019-11686, CVE-2019-11769, CVE-2019-11820, CVE-2019-11885, CVE-2019-12046, CVE-2019-12171, CVE-2019-12423, CVE-2019-12452, CVE-2019-12847, CVE-2019-13023, CVE-2019-13054, CVE-2019-13179, CVE-2019-13348, CVE-2019-13349, CVE-2019-13394, CVE-2019-13400, CVE-2019-1384, CVE-2019-14477, CVE-2019-14480, CVE-2019-14709, CVE-2019-14929, CVE-2019-15052, CVE-2019-15635, CVE-2019-15653, CVE-2019-15655, CVE-2019-15656, CVE-2019-16067, CVE-2019-16211, CVE-2019-16542, CVE-2019-16543, CVE-2019-16544, CVE-2019-16556, CVE-2019-16557, CVE-2019-16572, CVE-2019-16649, CVE-2019-16672, CVE-2019-16673, CVE-2019-17356, CVE-2019-17393, CVE-2019-17497, CVE-2019-17662, CVE-2019-18256, CVE-2019-18572, CVE-2019-18615, CVE-2019-18785, CVE-2019-18868, CVE-2019-19096, CVE-2019-19105, CVE-2019-19119, CVE-2019-19218, CVE-2019-19310, CVE-2019-19539, CVE-2019-19687, CVE-2019-19696, CVE-2019-19823, CVE-2019-19843, CVE-2019-19890, CVE-2019-19898, CVE-2019-20047, CVE-2019-25030, CVE-2019-3431, CVE-2019-3663, CVE-2019-3753, CVE-2019-3780, CVE-2019-3782, CVE-2019-3942, CVE-2019-3947, CVE-2019-4059, CVE-2019-4138, CVE-2019-4239, CVE-2019-4307, CVE-2019-4335, CVE-2019-4385, CVE-2019-4508, CVE-2019-4668, CVE-2019-4693, CVE-2019-4697, CVE-2019-4723, CVE-2019-4724, CVE-2019-5505, CVE-2019-5534, CVE-2019-5615, CVE-2019-5625, CVE-2019-5626, CVE-2019-5627, CVE-2019-5648, CVE-2019-5723, CVE-2019-5990, CVE-2019-6024, CVE-2019-6242, CVE-2019-6452, CVE-2019-6549, CVE-2019-6567, CVE-2019-6609, CVE-2019-6700, CVE-2019-7260, CVE-2019-7271, CVE-2019-7300, CVE-2019-8350, CVE-2019-8932, CVE-2019-9104, CVE-2019-9657, CVE-2019-9823, CVE-2019-9867, CVE-2019-9868, CVE-2019-9872, CVE-2019-9873
	2020	150	CVE-2020-0540, CVE-2020-10287, CVE-2020-10554, CVE-2020-10609, CVE-2020-10727, CVE-2020-10752, CVE-2020-10755, CVE-2020-11008, CVE-2020-11449, CVE-2020-11555, CVE-2020-11557, CVE-2020-11560, CVE-2020-11629, CVE-2020-11681, CVE-2020-11694, CVE-2020-11821, CVE-2020-11925, CVE-2020-12061, CVE-2020-12273, CVE-2020-12309, CVE-2020-12316, CVE-2020-12333, CVE-2020-12732, CVE-2020-12734, CVE-2020-13344, CVE-2020-13528, CVE-2020-13915, CVE-2020-14334, CVE-2020-14391, CVE-2020-14489, CVE-2020-14930, CVE-2020-15054, CVE-2020-15058, CVE-2020-15062, CVE-2020-15157, CVE-2020-15381, CVE-2020-15661, CVE-2020-15791, CVE-2020-16280, CVE-2020-1669, CVE-2020-16839, CVE-2020-17489, CVE-2020-1978, CVE-2020-2078, CVE-2020-2107, CVE-2020-2114, CVE-2020-2119, CVE-2020-2124, CVE-2020-2125, CVE-2020-2126, CVE-2020-2127, CVE-2020-2128, CVE-2020-2129, CVE-2020-2130, CVE-2020-2131, CVE-2020-2132, CVE-2020-2133, CVE-2020-2145, CVE-2020-2164, CVE-2020-2165, CVE-2020-2181, CVE-2020-2182, CVE-2020-2198, CVE-2020-21994, CVE-2020-2208, CVE-2020-2209, CVE-2020-2212, CVE-2020-2213, CVE-2020-2218, CVE-2020-2291, CVE-2020-2297, CVE-2020-23036, CVE-2020-2312, CVE-2020-2314, CVE-2020-2318, CVE-2020-2319, CVE-2020-24227, CVE-2020-24622, CVE-2020-24680, CVE-2020-25175, CVE-2020-25235, CVE-2020-25566, CVE-2020-26079, CVE-2020-26149, CVE-2020-26508, CVE-2020-26515, CVE-2020-27258, CVE-2020-27270, CVE-2020-27413, CVE-2020-27554, CVE-2020-27557, CVE-2020-27688, CVE-2020-27781, CVE-2020-27839, CVE-2020-27888, CVE-2020-28219, CVE-2020-28330, CVE-2020-28390, CVE-2020-29005, CVE-2020-29054, CVE-2020-29321, CVE-2020-29322, CVE-2020-29323, CVE-2020-29380, CVE-2020-3180, CVE-2020-3391, CVE-2020-3483, CVE-2020-35454, CVE-2020-35455, CVE-2020-3547, CVE-2020-35580, CVE-2020-3841, CVE-2020-4095, CVE-2020-4372, CVE-2020-4408, CVE-2020-4568, CVE-2020-4593, CVE-2020-4602, CVE-2020-4913, CVE-2020-5260, CVE-2020-5263, CVE-2020-5315, CVE-2020-5404, CVE-2020-5406, CVE-2020-5721, CVE-2020-5899, CVE-2020-6195, CVE-2020-6239, CVE-2020-6794, CVE-2020-6874, CVE-2020-6961, CVE-2020-6969, CVE-2020-7196, CVE-2020-7233, CVE-2020-7299, CVE-2020-7306, CVE-2020-7307, CVE-2020-7909, CVE-2020-7945, CVE-2020-8152, CVE-2020-8183, CVE-2020-8210, CVE-2020-8259, CVE-2020-8968, CVE-2020-9306, CVE-2020-9324, CVE-2020-9403, CVE-2020-9404, CVE-2020-9523, CVE-2020-9525

	2021	114	CVE-2021-0220, CVE-2021-1126, CVE-2021-1392, CVE-2021-1537, CVE-2021-1589, CVE-2021-1873, CVE-2021-20146, CVE-2021-20163, CVE-2021-20164, CVE-2021-20168, CVE-2021-20228, CVE-2021-20389, CVE-2021-20415, CVE-2021-20434, CVE-2021-20439, CVE-2021-20445, CVE-2021-20597, CVE-2021-20826, CVE-2021-20997, CVE-2021-21448, CVE-2021-21505, CVE-2021-21522, CVE-2021-21612, CVE-2021-21614, CVE-2021-21634, CVE-2021-21681, CVE-2021-22115, CVE-2021-22132, CVE-2021-22324, CVE-2021-22351, CVE-2021-22370, CVE-2021-22681, CVE-2021-22737, CVE-2021-22778, CVE-2021-22780, CVE-2021-22781, CVE-2021-22923, CVE-2021-23019, CVE-2021-23196, CVE-2021-23207, CVE-2021-23858, CVE-2021-26905, CVE-2021-27187, CVE-2021-27372, CVE-2021-27392, CVE-2021-27485, CVE-2021-27491, CVE-2021-27495, CVE-2021-27734, CVE-2021-28171, CVE-2021-28499, CVE-2021-28857, CVE-2021-29138, CVE-2021-29253, CVE-2021-29255, CVE-2021-29262, CVE-2021-29811, CVE-2021-30116, CVE-2021-30167, CVE-2021-3130, CVE-2021-3131, CVE-2021-3141, CVE-2021-3154, CVE-2021-3179, CVE-2021-31857, CVE-2021-32003, CVE-2021-32039, CVE-2021-3252, CVE-2021-32770, CVE-2021-3344, CVE-2021-34204, CVE-2021-34560, CVE-2021-34700, CVE-2021-34733, CVE-2021-35033, CVE-2021-35050, CVE-2021-3528, CVE-2021-35495, CVE-2021-35527, CVE-2021-35529, CVE-2021-35965, CVE-2021-36170, CVE-2021-36178, CVE-2021-36317, CVE-2021-36318, CVE-2021-37075, CVE-2021-37187, CVE-2021-37400, CVE-2021-37401, CVE-2021-37452, CVE-2021-3787, CVE-2021-38150, CVE-2021-38165, CVE-2021-38179, CVE-2021-38460, CVE-2021-38502, CVE-2021-38863, CVE-2021-39342, CVE-2021-39458, CVE-2021-40503, CVE-2021-40520, CVE-2021-40654, CVE-2021-40655, CVE-2021-40857, CVE-2021-41092, CVE-2021-41297, CVE-2021-41300, CVE-2021-41972, CVE-2021-42023, CVE-2021-42557, CVE-2021-43327, CVE-2021-43978, CVE-2021-45077, CVE-2021-45457
CWE-640	2019	16	CVE-2019-10270, CVE-2019-10641, CVE-2019-11393, CVE-2019-11414, CVE-2019-12476, CVE-2019-12943, CVE-2019-13240, CVE-2019-14955, CVE-2019-15749, CVE-2019-15929, CVE-2019-17392, CVE-2019-18818, CVE-2019-19844, CVE-2019-20004, CVE-2019-3787, CVE-2019-6560
	2020	10	CVE-2020-11027, CVE-2020-14015, CVE-2020-14016, CVE-2020-25105, CVE-2020-25728, CVE-2020-27179, CVE-2020-27408, CVE-2020-28186, CVE-2020-5361, CVE-2020-7245
	2021	23	CVE-2021-22731, CVE-2021-22763, CVE-2021-25323, CVE-2021-25957, CVE-2021-25961, CVE-2021-27651, CVE-2021-28128, CVE-2021-28293, CVE-2021-29080, CVE-2021-31912, CVE-2021-32648, CVE-2021-33321, CVE-2021-36095, CVE-2021-36209, CVE-2021-36708, CVE-2021-36804, CVE-2021-37541, CVE-2021-37693, CVE-2021-39899, CVE-2021-39919, CVE-2021-41694, CVE-2021-44037, CVE-2021-44839
CWE-798	2019	125	CVE-2019-0020, CVE-2019-0022, CVE-2019-10011, CVE-2019-10479, CVE-2019-10688, CVE-2019-10694, CVE-2019-10712, CVE-2019-10850, CVE-2019-10851, CVE-2019-10881, CVE-2019-10920, CVE-2019-10979, CVE-2019-10990, CVE-2019-10995, CVE-2019-11030, CVE-2019-11898, CVE-2019-11946, CVE-2019-11947, CVE-2019-12327, CVE-2019-12376, CVE-2019-12549, CVE-2019-12550, CVE-2019-12776, CVE-2019-12797, CVE-2019-12920, CVE-2019-13352, CVE-2019-13399, CVE-2019-13466, CVE-2019-13473, CVE-2019-13474, CVE-2019-13530, CVE-2019-13543, CVE-2019-13553, CVE-2019-13559, CVE-2019-13657, CVE-2019-13658, CVE-2019-14309, CVE-2019-14482, CVE-2019-14837, CVE-2019-14919, CVE-2019-14926, CVE-2019-14930, CVE-2019-14943, CVE-2019-15015, CVE-2019-15017, CVE-2019-15075, CVE-2019-15497, CVE-2019-15745, CVE-2019-15801, CVE-2019-15802, CVE-2019-15867, CVE-2019-15975, CVE-2019-15976, CVE-2019-15977, CVE-2019-16150, CVE-2019-16153, CVE-2019-1619, CVE-2019-16207, CVE-2019-16313, CVE-2019-16399, CVE-2019-16734, CVE-2019-1675, CVE-2019-1688, CVE-2019-17098, CVE-2019-1723, CVE-2019-18831, CVE-2019-19017, CVE-2019-19021, CVE-2019-19033, CVE-2019-19108, CVE-2019-1919, CVE-2019-1935, CVE-2019-19492, CVE-2019-20025, CVE-2019-20471, CVE-2019-20656, CVE-2019-25021, CVE-2019-3496, CVE-2019-3497, CVE-2019-3710, CVE-2019-3906, CVE-2019-3908, CVE-2019-3918, CVE-2019-3932, CVE-2019-3938, CVE-2019-3939, CVE-2019-3950, CVE-2019-3983, CVE-2019-4220, CVE-2019-4309, CVE-2019-4327, CVE-2019-4392, CVE-2019-4675, CVE-2019-4694, CVE-2019-5021, CVE-2019-5106, CVE-2019-5137, CVE-2019-5139, CVE-2019-5158, CVE-2019-5622, CVE-2019-6499, CVE-2019-6548, CVE-2019-6572, CVE-2019-6693, CVE-2019-6698, CVE-2019-6725, CVE-2019-6812, CVE-2019-6859, CVE-2019-7161, CVE-2019-7212, CVE-2019-7225, CVE-2019-7261, CVE-2019-7265, CVE-2019-7279, CVE-2019-7593, CVE-2019-7594, CVE-2019-7672, CVE-2019-8352, CVE-2019-8950, CVE-2019-9160, CVE-2019-9229, CVE-2019-9493, CVE-2019-9533, CVE-2019-9975, CVE-2019-9733

	2020	173	CVE-2020-0016, CVE-2020-0688, CVE-2020-10206, CVE-2020-10207, CVE-2020-10210, CVE-2020-10269, CVE-2020-10270, CVE-2020-10276, CVE-2020-10788, CVE-2020-10884, CVE-2020-10988, CVE-2020-10996, CVE-2020-11483, CVE-2020-11487, CVE-2020-11543, CVE-2020-11549, CVE-2020-11615, CVE-2020-11719, CVE-2020-11720, CVE-2020-11723, CVE-2020-11854, CVE-2020-11857, CVE-2020-11878, CVE-2020-11951, CVE-2020-12012, CVE-2020-12016, CVE-2020-12035, CVE-2020-12039, CVE-2020-12045, CVE-2020-12047, CVE-2020-12110, CVE-2020-12376, CVE-2020-12501, CVE-2020-12627, CVE-2020-12789, CVE-2020-13166, CVE-2020-13414, CVE-2020-13793, CVE-2020-13804, CVE-2020-13858, CVE-2020-14099, CVE-2020-14474, CVE-2020-14510, CVE-2020-15312, CVE-2020-15313, CVE-2020-15314, CVE-2020-15315, CVE-2020-15316, CVE-2020-15317, CVE-2020-15318, CVE-2020-15319, CVE-2020-15320, CVE-2020-15321, CVE-2020-15322, CVE-2020-15323, CVE-2020-15324, CVE-2020-15382, CVE-2020-15833, CVE-2020-1614, CVE-2020-1615, CVE-2020-16170, CVE-2020-16258, CVE-2020-1716, CVE-2020-1764, CVE-2020-21995, CVE-2020-24053, CVE-2020-24056, CVE-2020-24115, CVE-2020-24215, CVE-2020-24218, CVE-2020-24574, CVE-2020-24620, CVE-2020-24876, CVE-2020-2499, CVE-2020-2500, CVE-2020-25173, CVE-2020-25231, CVE-2020-25233, CVE-2020-25234, CVE-2020-25256, CVE-2020-25493, CVE-2020-25561, CVE-2020-25565, CVE-2020-25620, CVE-2020-25688, CVE-2020-25749, CVE-2020-25752, CVE-2020-26097, CVE-2020-26509, CVE-2020-26879, CVE-2020-26892, CVE-2020-27181, CVE-2020-27256, CVE-2020-27278, CVE-2020-27689, CVE-2020-28329, CVE-2020-28334, CVE-2020-28391, CVE-2020-28395, CVE-2020-28952, CVE-2020-28998, CVE-2020-28999, CVE-2020-29059, CVE-2020-29060, CVE-2020-29061, CVE-2020-29062, CVE-2020-29193, CVE-2020-29375, CVE-2020-29376, CVE-2020-29377, CVE-2020-29382, CVE-2020-29383, CVE-2020-3158, CVE-2020-3165, CVE-2020-3234, CVE-2020-3301, CVE-2020-3318, CVE-2020-3330, CVE-2020-3382, CVE-2020-3446, CVE-2020-35138, CVE-2020-35296, CVE-2020-35338, CVE-2020-35567, CVE-2020-35929, CVE-2020-3928, CVE-2020-4177, CVE-2020-4190, CVE-2020-4208, CVE-2020-4216, CVE-2020-4269, CVE-2020-4283, CVE-2020-4385, CVE-2020-4429, CVE-2020-4459, CVE-2020-4622, CVE-2020-4690, CVE-2020-4854, CVE-2020-4932, CVE-2020-4983, CVE-2020-5222, CVE-2020-5248, CVE-2020-5349, CVE-2020-5351, CVE-2020-5374, CVE-2020-5667, CVE-2020-6265, CVE-2020-6779, CVE-2020-6857, CVE-2020-6882, CVE-2020-6963, CVE-2020-6979, CVE-2020-6981, CVE-2020-6983, CVE-2020-6985, CVE-2020-6990, CVE-2020-7498, CVE-2020-7501, CVE-2020-7515, CVE-2020-7590, CVE-2020-7846, CVE-2020-7999, CVE-2020-8000, CVE-2020-8001, CVE-2020-8573, CVE-2020-8657, CVE-2020-8868, CVE-2020-8964, CVE-2020-8995, CVE-2020-9279, CVE-2020-9289, CVE-2020-9306, CVE-2020-9435
	2021	139	CVE-2021-0245, CVE-2021-0248, CVE-2021-0266, CVE-2021-0279, CVE-2021-1219, CVE-2021-1574, CVE-2021-20025, CVE-2021-20132, CVE-2021-20155, CVE-2021-20170, CVE-2021-20401, CVE-2021-20412, CVE-2021-20426, CVE-2021-20442, CVE-2021-20537, CVE-2021-20612, CVE-2021-20748, CVE-2021-21818, CVE-2021-21820, CVE-2021-21913, CVE-2021-22667, CVE-2021-22707, CVE-2021-22729, CVE-2021-22730, CVE-2021-23233, CVE-2021-23842, CVE-2021-24005, CVE-2021-25275, CVE-2021-25863, CVE-2021-25898, CVE-2021-26108, CVE-2021-26611, CVE-2021-27141, CVE-2021-27142, CVE-2021-27143, CVE-2021-27144, CVE-2021-27145, CVE-2021-27146, CVE-2021-27147, CVE-2021-27148, CVE-2021-27149, CVE-2021-27150, CVE-2021-27151, CVE-2021-27152, CVE-2021-27153, CVE-2021-27154, CVE-2021-27155, CVE-2021-27156, CVE-2021-27157, CVE-2021-27158, CVE-2021-27159, CVE-2021-27160, CVE-2021-27161, CVE-2021-27162, CVE-2021-27163, CVE-2021-27164, CVE-2021-27165, CVE-2021-27166, CVE-2021-27167, CVE-2021-27168, CVE-2021-27169, CVE-2021-27172, CVE-2021-27228, CVE-2021-27254, CVE-2021-27389, CVE-2021-27437, CVE-2021-27438, CVE-2021-27440, CVE-2021-27452, CVE-2021-27481, CVE-2021-27503, CVE-2021-27952, CVE-2021-28111, CVE-2021-28123, CVE-2021-28152, CVE-2021-28912, CVE-2021-29691, CVE-2021-29728, CVE-2021-30165, CVE-2021-31477, CVE-2021-31505, CVE-2021-31579, CVE-2021-32454, CVE-2021-32459, CVE-2021-32520, CVE-2021-32521, CVE-2021-32525, CVE-2021-32535, CVE-2021-32588, CVE-2021-32993, CVE-2021-33218, CVE-2021-33219, CVE-2021-33220, CVE-2021-33484, CVE-2021-33529, CVE-2021-33531, CVE-2021-33540, CVE-2021-33583, CVE-2021-34565, CVE-2021-34571, CVE-2021-34795, CVE-2021-34812, CVE-2021-35232, CVE-2021-35961, CVE-2021-36234, CVE-2021-36312, CVE-2021-36751, CVE-2021-36799, CVE-2021-37163, CVE-2021-37555, CVE-2021-38456, CVE-2021-38461, CVE-2021-39245, CVE-2021-39613, CVE-2021-39614, CVE-2021-39615, CVE-2021-40119, CVE-2021-40494, CVE-2021-40519, CVE-2021-41028, CVE-2021-41299, CVE-2021-41320, CVE-2021-41827, CVE-2021-41828, CVE-2021-43044, CVE-2021-43052, CVE-2021-43282, CVE-2021-43284, CVE-2021-43552, CVE-2021-43575, CVE-2021-43587, CVE-2021-44207, CVE-2021-44464, CVE-2021-45033, CVE-2021-45520, CVE-2021-45521, CVE-2021-45522, CVE-2021-45732, CVE-2021-45913
CWE-261	2019	0	
	2020	1	CVE-2020-10919
	2021	0	
CWE-303	2019	0	
	2020	1	CVE-2020-15632
	2021	2	CVE-2021-21378, CVE-2021-25315
CWE-603	2019	0	
	2020	1	CVE-2020-7591
	2021	0	
CWE-302	2019	0	
	2020	0	
	2021	1	CVE-2021-1399
CWE-304	2019	0	
	2020	0	
	2021	1	CVE-2021-41179
CWE-620	2019	0	
	2020	0	
	2021	1	CVE-2021-22773

CWE-287	2019	239	CVE-2019-0282, CVE-2019-0543, CVE-2019-0622, CVE-2019-10150, CVE-2019-10157, CVE-2019-1020018, CVE-2019-10273, CVE-2019-10562, CVE-2019-10643, CVE-2019-10661, CVE-2019-10689, CVE-2019-10884, CVE-2019-10911, CVE-2019-10964, CVE-2019-10966, CVE-2019-10998, CVE-2019-11015, CVE-2019-11018, CVE-2019-11064, CVE-2019-11081, CVE-2019-11170, CVE-2019-11187, CVE-2019-11202, CVE-2019-11232, CVE-2019-11234, CVE-2019-11488, CVE-2019-11576, CVE-2019-11733, CVE-2019-12300, CVE-2019-12394, CVE-2019-12395, CVE-2019-12405, CVE-2019-12440, CVE-2019-12530, CVE-2019-12564, CVE-2019-12643, CVE-2019-12664, CVE-2019-12845, CVE-2019-13188, CVE-2019-13190, CVE-2019-13294, CVE-2019-13336, CVE-2019-13361, CVE-2019-13372, CVE-2019-13526, CVE-2019-14238, CVE-2019-14239, CVE-2019-14432, CVE-2019-14510, CVE-2019-14553, CVE-2019-14598, CVE-2019-14705, CVE-2019-14856, CVE-2019-14909, CVE-2019-14985, CVE-2019-15046, CVE-2019-15299, CVE-2019-15585, CVE-2019-15615, CVE-2019-15648, CVE-2019-15803, CVE-2019-15897, CVE-2019-15987, CVE-2019-15993, CVE-2019-16028, CVE-2019-16190, CVE-2019-16201, CVE-2019-16250, CVE-2019-16261, CVE-2019-16286, CVE-2019-16327, CVE-2019-1662, CVE-2019-1664, CVE-2019-1666, CVE-2019-16929, CVE-2019-17023, CVE-2019-17134, CVE-2019-1724, CVE-2019-17372, CVE-2019-17437, CVE-2019-1758, CVE-2019-1759, CVE-2019-17627, CVE-2019-18246, CVE-2019-18250, CVE-2019-18252, CVE-2019-18312, CVE-2019-18314, CVE-2019-18315, CVE-2019-18317, CVE-2019-18318, CVE-2019-18319, CVE-2019-18321, CVE-2019-18322, CVE-2019-18332, CVE-2019-18337, CVE-2019-18341, CVE-2019-18374, CVE-2019-18380, CVE-2019-1842, CVE-2019-18661, CVE-2019-1867, CVE-2019-1877, CVE-2019-18848, CVE-2019-18906, CVE-2019-19006, CVE-2019-1917, CVE-2019-1937, CVE-2019-1938, CVE-2019-1946, CVE-2019-19507, CVE-2019-19518, CVE-2019-19519, CVE-2019-19521, CVE-2019-19560, CVE-2019-19562, CVE-2019-19598, CVE-2019-1974, CVE-2019-1980, CVE-2019-19825, CVE-2019-19857, CVE-2019-19982, CVE-2019-20027, CVE-2019-20033, CVE-2019-20046, CVE-2019-20062, CVE-2019-2018, CVE-2019-20360, CVE-2019-20412, CVE-2019-20464, CVE-2019-20481, CVE-2019-20489, CVE-2019-20533, CVE-2019-20565, CVE-2019-20618, CVE-2019-20620, CVE-2019-20786, CVE-2019-20833, CVE-2019-20875, CVE-2019-20879, CVE-2019-20933, CVE-2019-3584, CVE-2019-3654, CVE-2019-3775, CVE-2019-3798, CVE-2019-3820, CVE-2019-3825, CVE-2019-3878, CVE-2019-3884, CVE-2019-3927, CVE-2019-3935, CVE-2019-3997, CVE-2019-3998, CVE-2019-5061, CVE-2019-5108, CVE-2019-5165, CVE-2019-5213, CVE-2019-5218, CVE-2019-5223, CVE-2019-5233, CVE-2019-5252, CVE-2019-5253, CVE-2019-5298, CVE-2019-5317, CVE-2019-5426, CVE-2019-5453, CVE-2019-5455, CVE-2019-5473, CVE-2019-5486, CVE-2019-5679, CVE-2019-5890, CVE-2019-5909, CVE-2019-5964, CVE-2019-6143, CVE-2019-6441, CVE-2019-6481, CVE-2019-6519, CVE-2019-6521, CVE-2019-6527, CVE-2019-6675, CVE-2019-6744, CVE-2019-6814, CVE-2019-6832, CVE-2019-7163, CVE-2019-7218, CVE-2019-7226, CVE-2019-7392, CVE-2019-7579, CVE-2019-7666, CVE-2019-8108, CVE-2019-8443, CVE-2019-8533, CVE-2019-8634, CVE-2019-8704, CVE-2019-8760, CVE-2019-8804, CVE-2019-8978, CVE-2019-8990, CVE-2019-9124, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, CVE-2019-9531, CVE-2019-9629, CVE-2019-10256, CVE-2019-19873, CVE-2019-19878, CVE-2019-20642, CVE-2019-20681, CVE-2019-20690, CVE-2019-20760, CVE-2019-4210, CVE-2019-4241, CVE-2019-5347, CVE-2019-5396, CVE-2019-7964, CVE-2019-8081, CVE-2019-0101, CVE-2019-0173, CVE-2019-11210, CVE-2019-12428, CVE-2019-13531, CVE-2019-13953, CVE-2019-15067, CVE-2019-15069, CVE-2019-15088, CVE-2019-18225, CVE-2019-19556, CVE-2019-20490, CVE-2019-20492, CVE-2019-20498, CVE-2019-3629, CVE-2019-3706, CVE-2019-3707, CVE-2019-3717, CVE-2019-3910, CVE-2019-5134, CVE-2019-9196

	2020	282	CVE-2020-0460, CVE-2020-10048, CVE-2020-10123, CVE-2020-10148, CVE-2020-10254, CVE-2020-10278, CVE-2020-10288, CVE-2020-10539, CVE-2020-10594, CVE-2020-10669, CVE-2020-10709, CVE-2020-10816, CVE-2020-10846, CVE-2020-10847, CVE-2020-10888, CVE-2020-10916, CVE-2020-10918, CVE-2020-11020, CVE-2020-11264, CVE-2020-11301, CVE-2020-11542, CVE-2020-11551, CVE-2020-11796, CVE-2020-11964, CVE-2020-11965, CVE-2020-12126, CVE-2020-12145, CVE-2020-12638, CVE-2020-12812, CVE-2020-12848, CVE-2020-12874, CVE-2020-13185, CVE-2020-13290, CVE-2020-13292, CVE-2020-13303, CVE-2020-13365, CVE-2020-13859, CVE-2020-13929, CVE-2020-13963, CVE-2020-14070, CVE-2020-14158, CVE-2020-14299, CVE-2020-14380, CVE-2020-14455, CVE-2020-14477, CVE-2020-14485, CVE-2020-15027, CVE-2020-15055, CVE-2020-15059, CVE-2020-15063, CVE-2020-15077, CVE-2020-15078, CVE-2020-15149, CVE-2020-15482, CVE-2020-15601, CVE-2020-15605, CVE-2020-15802, CVE-2020-15835, CVE-2020-15896, CVE-2020-15921, CVE-2020-15949, CVE-2020-16088, CVE-2020-16169, CVE-2020-1618, CVE-2020-16222, CVE-2020-16239, CVE-2020-16251, CVE-2020-1637, CVE-2020-1718, CVE-2020-17510, CVE-2020-17523, CVE-2020-1778, CVE-2020-1786, CVE-2020-1787, CVE-2020-1788, CVE-2020-1789, CVE-2020-1793, CVE-2020-1794, CVE-2020-1798, CVE-2020-1801, CVE-2020-1803, CVE-2020-1812, CVE-2020-1833, CVE-2020-1838, CVE-2020-1840, CVE-2020-1842, CVE-2020-1864, CVE-2020-1878, CVE-2020-19003, CVE-2020-19037, CVE-2020-19419, CVE-2020-19888, CVE-2020-2018, CVE-2020-2050, CVE-2020-21932, CVE-2020-21934, CVE-2020-21991, CVE-2020-22001, CVE-2020-2299, CVE-2020-2300, CVE-2020-2301, CVE-2020-23058, CVE-2020-23139, CVE-2020-24029, CVE-2020-24514, CVE-2020-24563, CVE-2020-24579, CVE-2020-24612, CVE-2020-24629, CVE-2020-24641, CVE-2020-24675, CVE-2020-24786, CVE-2020-24848, CVE-2020-24987, CVE-2020-25165, CVE-2020-25183, CVE-2020-25218, CVE-2020-25251, CVE-2020-25592, CVE-2020-25848, CVE-2020-25867, CVE-2020-26030, CVE-2020-26101, CVE-2020-26105, CVE-2020-26136, CVE-2020-26139, CVE-2020-26160, CVE-2020-26168, CVE-2020-26200, CVE-2020-26214, CVE-2020-26236, CVE-2020-26511, CVE-2020-26542, CVE-2020-26558, CVE-2020-26834, CVE-2020-26921, CVE-2020-27199, CVE-2020-27254, CVE-2020-27266, CVE-2020-27488, CVE-2020-27558, CVE-2020-27780, CVE-2020-27838, CVE-2020-28002, CVE-2020-28050, CVE-2020-28333, CVE-2020-28638, CVE-2020-28874, CVE-2020-28896, CVE-2020-28940, CVE-2020-28970, CVE-2020-28971, CVE-2020-29127, CVE-2020-29378, CVE-2020-29392, CVE-2020-29563, CVE-2020-29633, CVE-2020-29668, CVE-2020-29669, CVE-2020-3125, CVE-2020-3144, CVE-2020-3151, CVE-2020-3197, CVE-2020-3216, CVE-2020-3297, CVE-2020-3361, CVE-2020-3388, CVE-2020-3410, CVE-2020-3411, CVE-2020-35207, CVE-2020-35208, CVE-2020-35219, CVE-2020-35231, CVE-2020-3565, CVE-2020-35758, CVE-2020-35785, CVE-2020-36125, CVE-2020-36176, CVE-2020-3923, CVE-2020-3944, CVE-2020-3952, CVE-2020-4074, CVE-2020-4167, CVE-2020-4205, CVE-2020-4427, CVE-2020-4494, CVE-2020-4662, CVE-2020-4670, CVE-2020-4747, CVE-2020-4771, CVE-2020-4779, CVE-2020-4821, CVE-2020-4879, CVE-2020-5148, CVE-2020-5206, CVE-2020-5268, CVE-2020-5384, CVE-2020-5425, CVE-2020-5532, CVE-2020-5536, CVE-2020-5563, CVE-2020-5567, CVE-2020-5608, CVE-2020-5616, CVE-2020-5633, CVE-2020-5686, CVE-2020-5727, CVE-2020-5777, CVE-2020-5849, CVE-2020-5860, CVE-2020-6091, CVE-2020-6871, CVE-2020-6988, CVE-2020-7197, CVE-2020-7199, CVE-2020-7222, CVE-2020-7276, CVE-2020-7293, CVE-2020-7294, CVE-2020-7295, CVE-2020-7296, CVE-2020-7297, CVE-2020-7323, CVE-2020-7378, CVE-2020-7787, CVE-2020-7856, CVE-2020-8097, CVE-2020-8108, CVE-2020-8148, CVE-2020-8200, CVE-2020-8206, CVE-2020-8207, CVE-2020-8236, CVE-2020-8253, CVE-2020-8267, CVE-2020-8272, CVE-2020-8350, CVE-2020-8465, CVE-2020-8510, CVE-2020-8558, CVE-2020-8591, CVE-2020-8595, CVE-2020-8606, CVE-2020-8664, CVE-2020-8685, CVE-2020-8708, CVE-2020-8709, CVE-2020-8713, CVE-2020-8714, CVE-2020-8771, CVE-2020-8828, CVE-2020-8861, CVE-2020-8862, CVE-2020-8863, CVE-2020-8953, CVE-2020-8994, CVE-2020-9049, CVE-2020-9064, CVE-2020-9066, CVE-2020-9068, CVE-2020-9070, CVE-2020-9073, CVE-2020-9076, CVE-2020-9077, CVE-2020-9099, CVE-2020-9109, CVE-2020-9207, CVE-2020-9233, CVE-2020-9259, CVE-2020-9277, CVE-2020-9294, CVE-2020-0943, CVE-2020-11445, CVE-2020-11788, CVE-2020-11989, CVE-2020-15506, CVE-2020-1957, CVE-2020-26926, CVE-2020-4493, CVE-2020-4499, CVE-2020-13933, CVE-2020-23355

	2021	358	CVE-2021-0096, CVE-2021-0570, CVE-2021-0571, CVE-2021-0572, CVE-2021-0649, CVE-2021-1468, CVE-2021-1541, CVE-2021-1543, CVE-2021-1561, CVE-2021-1579, CVE-2021-1591, CVE-2021-1600, CVE-2021-1601, CVE-2021-1862, CVE-2021-1863, CVE-2021-20018, CVE-2021-20020, CVE-2021-20107, CVE-2021-20145, CVE-2021-20150, CVE-2021-20158, CVE-2021-20288, CVE-2021-20372, CVE-2021-20375, CVE-2021-20578, CVE-2021-20590, CVE-2021-20593, CVE-2021-20598, CVE-2021-20630, CVE-2021-20632, CVE-2021-20634, CVE-2021-20737, CVE-2021-20757, CVE-2021-20759, CVE-2021-20776, CVE-2021-20861, CVE-2021-21125, CVE-2021-21126, CVE-2021-21127, CVE-2021-21129, CVE-2021-21130, CVE-2021-21131, CVE-2021-21133, CVE-2021-21141, CVE-2021-21177, CVE-2021-21189, CVE-2021-21308, CVE-2021-21329, CVE-2021-21335, CVE-2021-21513, CVE-2021-21538, CVE-2021-21564, CVE-2021-21745, CVE-2021-21902, CVE-2021-21952, CVE-2021-21953, CVE-2021-21955, CVE-2021-21982, CVE-2021-21986, CVE-2021-21994, CVE-2021-21998, CVE-2021-22002, CVE-2021-22004, CVE-2021-22025, CVE-2021-22057, CVE-2021-22171, CVE-2021-22228, CVE-2021-22473, CVE-2021-22490, CVE-2021-22496, CVE-2021-22497, CVE-2021-22507, CVE-2021-22566, CVE-2021-22764, CVE-2021-22858, CVE-2021-22860, CVE-2021-22893, CVE-2021-22943, CVE-2021-22997, CVE-2021-23008, CVE-2021-23147, CVE-2021-23365, CVE-2021-23857, CVE-2021-23923, CVE-2021-24017, CVE-2021-24148, CVE-2021-24175, CVE-2021-24527, CVE-2021-24647, CVE-2021-25036, CVE-2021-25147, CVE-2021-25281, CVE-2021-25341, CVE-2021-25342, CVE-2021-25343, CVE-2021-25368, CVE-2021-25389, CVE-2021-25424, CVE-2021-25430, CVE-2021-25442, CVE-2021-25445, CVE-2021-25446, CVE-2021-25447, CVE-2021-25448, CVE-2021-25451, CVE-2021-25466, CVE-2021-25484, CVE-2021-25505, CVE-2021-25910, CVE-2021-25956, CVE-2021-26070, CVE-2021-26077, CVE-2021-26088, CVE-2021-26117, CVE-2021-26118, CVE-2021-26697, CVE-2021-26923, CVE-2021-27173, CVE-2021-27215, CVE-2021-27451, CVE-2021-27610, CVE-2021-27668, CVE-2021-27791, CVE-2021-27794, CVE-2021-27876, CVE-2021-27877, CVE-2021-27878, CVE-2021-27990, CVE-2021-28024, CVE-2021-28093, CVE-2021-28094, CVE-2021-28095, CVE-2021-28122, CVE-2021-28124, CVE-2021-28131, CVE-2021-28148, CVE-2021-28174, CVE-2021-28493, CVE-2021-28494, CVE-2021-28495, CVE-2021-28626, CVE-2021-28694, CVE-2021-28958, CVE-2021-29047, CVE-2021-29065, CVE-2021-29066, CVE-2021-29067, CVE-2021-29149, CVE-2021-29151, CVE-2021-29203, CVE-2021-29487, CVE-2021-29747, CVE-2021-29758, CVE-2021-29765, CVE-2021-29779, CVE-2021-29908, CVE-2021-30158, CVE-2021-30302, CVE-2021-30312, CVE-2021-3046, CVE-2021-30605, CVE-2021-30640, CVE-2021-30648, CVE-2021-30667, CVE-2021-30668, CVE-2021-30702, CVE-2021-30720, CVE-2021-30769, CVE-2021-30770, CVE-2021-30867, CVE-2021-30948, CVE-2021-31245, CVE-2021-31251, CVE-2021-31349, CVE-2021-3145, CVE-2021-31520, CVE-2021-31606, CVE-2021-31917, CVE-2021-32030, CVE-2021-32033, CVE-2021-32071, CVE-2021-32541, CVE-2021-32543, CVE-2021-32579, CVE-2021-32637, CVE-2021-32646, CVE-2021-32691, CVE-2021-32693, CVE-2021-32729, CVE-2021-32738, CVE-2021-32794, CVE-2021-3282, CVE-2021-32951, CVE-2021-32967, CVE-2021-3297, CVE-2021-33044, CVE-2021-33045, CVE-2021-33046, CVE-2021-33087, CVE-2021-33210, CVE-2021-3325, CVE-2021-3339, CVE-2021-33539, CVE-2021-33700, CVE-2021-33766, CVE-2021-33831, CVE-2021-33842, CVE-2021-33843, CVE-2021-34166, CVE-2021-3424, CVE-2021-34546, CVE-2021-34578, CVE-2021-3458, CVE-2021-34675, CVE-2021-34676, CVE-2021-34690, CVE-2021-34746, CVE-2021-34785, CVE-2021-34786, CVE-2021-34865, CVE-2021-34977, CVE-2021-34993, CVE-2021-35029, CVE-2021-3519, CVE-2021-35296, CVE-2021-35324, CVE-2021-3547, CVE-2021-35528, CVE-2021-35941, CVE-2021-35973, CVE-2021-35979, CVE-2021-36124, CVE-2021-36128, CVE-2021-36306, CVE-2021-36350, CVE-2021-36370, CVE-2021-36560, CVE-2021-36721, CVE-2021-36745, CVE-2021-36921, CVE-2021-36949, CVE-2021-37043, CVE-2021-37054, CVE-2021-37100, CVE-2021-37123, CVE-2021-37151, CVE-2021-37153, CVE-2021-37172, CVE-2021-37254, CVE-2021-37331, CVE-2021-37414, CVE-2021-37415, CVE-2021-37420, CVE-2021-37545, CVE-2021-37580, CVE-2021-37597, CVE-2021-37624, CVE-2021-37736, CVE-2021-37741, CVE-2021-37927, CVE-2021-38137, CVE-2021-38161, CVE-2021-38412, CVE-2021-38513, CVE-2021-38514, CVE-2021-38618, CVE-2021-38686, CVE-2021-38688, CVE-2021-38696, CVE-2021-39119, CVE-2021-39138, CVE-2021-39165, CVE-2021-39177, CVE-2021-39196, CVE-2021-39215, CVE-2021-39226, CVE-2021-39236, CVE-2021-39296, CVE-2021-39872, CVE-2021-39890, CVE-2021-39916, CVE-2021-40130, CVE-2021-40350, CVE-2021-40380, CVE-2021-40539, CVE-2021-40684, CVE-2021-4073, CVE-2021-40826, CVE-2021-40851, CVE-2021-40856, CVE-2021-40866, CVE-2021-40867, CVE-2021-40996, CVE-2021-40997, CVE-2021-41126, CVE-2021-41157, CVE-2021-41265, CVE-2021-41286, CVE-2021-41303, CVE-2021-41308, CVE-2021-41309, CVE-2021-41311, CVE-2021-41312, CVE-2021-41314, CVE-2021-41317, CVE-2021-41393, CVE-2021-41503, CVE-2021-41580, CVE-2021-41716, CVE-2021-41753, CVE-2021-42072, CVE-2021-42338, CVE-2021-43068, CVE-2021-43136, CVE-2021-43175, CVE-2021-43183, CVE-2021-43203, CVE-2021-43355, CVE-2021-43415, CVE-2021-43563, CVE-2021-43786, CVE-2021-43833, CVE-2021-43834, CVE-2021-43931, CVE-2021-43946, CVE-2021-43999, CVE-2021-44077, CVE-2021-44152, CVE-2021-44420, CVE-2021-44458, CVE-2021-44514, CVE-2021-44515, CVE-2021-44524, CVE-2021-44526, CVE-2021-44675, CVE-2021-44757, CVE-2021-44848, CVE-2021-44949, CVE-2021-45495, CVE-2021-45496, CVE-2021-45497, CVE-2021-45498, CVE-2021-45499, CVE-2021-45500, CVE-2021-45501, CVE-2021-45502, CVE-2021-45503, CVE-2021-45504, CVE-2021-45505, CVE-2021-45506, CVE-2021-45507, CVE-2021-45508, CVE-2021-45509, CVE-2021-45510, CVE-2021-45511, CVE-2021-45890, CVE-2021-45917, CVE-2021-31924