HAAVOITTUVUUSPALKINTO-OHJELMAN SÄÄNNÖT JA EHDOT

Näitä sääntöjä ja ehtoja sovelletaan Verohallinnon haavoittuvuuspalkinto-ohjelmaan, joka järjestetään Hackrfi Oy:n palvelun kautta.

Tässä ohjelmassa tarkoituksena on havaita verotuksen kannalta kriittisiä tietoturvahaavoittuvuuksia Verohallinnon OmaVero-palvelussa (katso tarkemmin kohdasta ohjelman laajuus), joiden havaitsemisesta palkitaan. Tässä dokumentissa olevia sääntöjä ja ehtoja sovelletaan Verohallinnon OmaVero -haavoittuvuuspalkinto-ohjelmaan. Epäselvyyksien ja turhan työn välttämiseksi suosittelemme, että seuraavan ohjeistuksen tutustutaan huolellisesti ennen ohjelmaan osallistumista.

OHJELMASTAMME YLEISESTI

Kannustaaksemme tietoturvaongelmien löytämiseen ja julkaisemiseen vastuullisella ja läpinäkyvällä tavalla tarjoamme palkintoja hyväksytyistä tietoturvahaavoittuvuuksista, jotka raportoidaan meille Hackrfi-palvelun kautta. Tietoturvahaavoittuvuudeksi luokitellaan tapahtuma, joka yleisen termistön mukaisesti aiheuttaa häiriön tiedon tai palvelun luottamuksellisuudelle, eheydelle tai saatavuudelle. Tässä dokumentissa annettuja sääntöjä on noudatettava, jotta haavoittuvuuspalkinto-ohjelmaan osallistuminen ja siihen liittyvän tietoturvatutkimuksen suorittaminen ei aiheuta ennalta arvaamattomia tietoturvariskejä Verohallinnon asiakkaille, asiakastiedoille tai verotuksen toiminnalle.

OHJELMAN LAAJUUS

Kohde on WWW-pohjainen OmaVero-palvelu sekä 2.1.2018 alkaen sen palvelin osoitteissa:

URL: https://www.vero.fi/omavero/
IP: 131.207.14.14

Palvelussa oleva oikaisuvaatimusten lähettämistoiminto on rajattu ohjelmasta ulos, koska järjestelmä on tuotannossa ja toimintoa ei voi peruuttaa. Älä testaa sitä.

Palvelun tarkoitus: OmaVerosta on tulossa Verohallinnon pääasiallinen sähköinen palvelukanava, jonka toiminnallisuutta lisätään vaihe kerrallaan. Marraskuussa 2018 sinne lisätään uusia toimintoja, mm. verokorttien hakemista, ennakkoverojen käsittelyä, ilmoitusten antamista ja käsittelyä.

Mistä olemme erityisesti kiinnostuneita: Tietojen vuotaminen suuressa mittakaavassa, muiden asiakkaiden tietojen näkyminen tai muuttaminen, sekä yksityisyyden suojaan liittyvät ongelmat.

Sovelluksen käyttö edellyttää tunnistusta Väestörekisterikeskuksen (VRK) tuottaman *tunnistaminen.suomi.fi* palvelun kautta, jonka käyttö vaatii suomalaiset pankkitunnukset tai sähköisen henkilökortin. VRK:n tunnistus- ja valtuutuspalvelu eivät ole tämän haavoittuvuuspalkkio-ohjelman piirissä. Jos VRK:lla on käynnissä oma haavoittuvuuspalkkio-ohjelma, tunnistukseen ja valtuutukseen liittyvät ongelmat voidaan raportoida sinne ja palkkio voidaan maksaa joko Verohallinnon tai VRK:n ohjelmasta riippuen siitä kumpi on vastuussa haavoittuvasta osiosta. Yhdestä haavoittuvuudesta maksetaan kuitenkin aina vain yksi palkkio.

PERIAATTEELLISET RAJAUKSET

Arvostamme sitä, että saamme toimia raportoijien kanssa yhteistyössä palvelumme tietoturvallisuuden parantamiseksi ja toivomme myös saavuttavamme sekä hakkeri- että tietoturvayhteisössä luottamusta ratkaisuumme. Kunnioitamme raportoijan tähän käyttämää aikaa, ja toivomme siksi myös raportoijan kunnioittavan meidän palvelu-, vaste- ja korjausaikojamme.

- **Lain kunnioitus**: Tietoturvatutkimuksessa on noudatettava Suomen lakia ja näitä sääntöjä.
- **Riippumattomuus**: Haavoittuvuuspalkinto-ohjelmaan osallistuja ei saa olla Verohallinnon palveluksessa tai osallistunut OmaVero-palvelun toteutukseen tai sen tietoturvatarkastuksen tekemiseen.
- **Tutkijan oma toiminta**: Tietoturvatutkimus on suoritettava tutkijan itse omistamalta ja ylläpitämältä laitteelta tai laitteilta.
- **Vahingon rajoittaminen**: Tietoturvatutkimuksessa ei saa käyttää haitallista tai häiriötä aiheuttavaa kuormaa tai syötettä sen enempää kuin mitä teknisen tietoturvahaavoittuvuuden olemassaolon todentaminen edellyttää.
- **Verotuksen salliminen**: Tietoturvatutkimuksen suorittaminen ei saa merkittävällä tavalla vaikuttaa ohjelman kohteena olevan palvelun saatavuuteen.
- **Salassapito**: Jos löytyy haavoittuvuus, jonka vuoksi saadaan näkyville sellaista tietoa, joka ei olisi ilman haavoittuvuutta mahdollista, on raportoijan pidettävä tällä tavoin saamansa tiedot salassa välittämättä tai ilmaisematta niitä kolmansille osapuolille.
- Epäselvissä tilanteissa pyydämme olemaan meihin yhteydessä osoitteen https://www.hackr.fi kautta ennen ohjelmaan osallistumista.

KIELLETYT TOIMET JA MENETELMÄT

Seuraavien toimien suorittaminen johtaa haavoittuvuuspalkinto-ohjelmaan osallistumisen hylkäykseen sekä mahdollisesti viranomaistoimiin toimien luonteesta riippuen:

- Koodi-injektiot (esimerkiksi SQL-injektio) taustajärjestelmiin siten että järjestelmässä tai taustajärjestelmässä olevia tietoja **muutetaan** tai **poistetaan**. Tietojen luku tällä menetelmällä on sallittua ja riittää osoittamaan ongelman olemassaolon.
- Palvelunestohyökkäykset ("DoS"- Denial of Service) - tämä koskettaa myös automaattisia skannereita ja muita työkaluja, joiden käytöstä saattaa syntyä palvelunestohyökkäyksen kaltaista kuormaa.
- Ns. ”social engineering” sekä fyysiset hyökkäykset kuten MitM-hyökkäykset.
- Yksilön turvallisuuden uhkaaminen.
- Verotuksen toimintaa haittaavat (tai suurella todennäköisyydellä haittaavat) toimet tulee jättää suorittamatta tämän ohjelman piirissä oleviin tai sen ulkopuolella oleviin järjestelmiin.
- Siirtyminen muihin palvelimiin (ns. ”pivot”). Muihin palvelimiin kuin kohteeseen siirtyminen on luvanvaraista. Jos pääset murtautumaan kohdepalvelimelle, ota yhteyttä Hackrfi:n asiantuntijoihin, niin selvitämme luvan kokeilla muihin palvelimiin siirtymistä.

HAAVOITTUVUUDEN RAPORTOINTI

Havaittu haavoittuvuus on raportoitava osoitteessa http://www.hackr.fi olevan ohjelmasivun oman raportointilomakkeen kautta.

Seuraavassa on raportointiin liittyviä yksityiskohtia:

- Raportoijan on jaettava kaikki mahdollinen tieto ja yksityiskohdat, jotta haavoittuvuus voidaan todentaa. Jos havaintoa ei voida toistaa, ei myöskään palkkiota voida tarjota. Tietoa ei saa jättää pois raportista mahdollista myöhempää raporttien tai havaintojen ketjuttamista varten.
- Pyrimme olemaan raportoijaan yhteydessä keskimäärin 3 työpäivän kuluessa havainnosta kertoaksemme raportin käsittelyn etenemisestä.
- Pyrimme vahvistamaan raportin oikeellisuuden keskimäärin 14 työpäivän sisällä. Pyydämme kuitenkin huomioimaan, että raportista riippuen sen vahvistaminen saattaa kestää tätä pitempään. Vahvistamiseen kuluva aika riippuu myös raportin kattavuudesta sekä havainnon toistamisen helppoudesta.
- Tutkimustyö ei saa uhata tai vaarantaa muita palvelun käyttäjiä. Jos raportoijalla on epäilys, että seuraava askel tutkimuksessa aiheuttaa palveluun häiriöitä, voidaan raportti toimittaa keskeneräisenä, ja hakea etukäteen lupa tutkimusten jatkamiseen.
- Liitteet ja liitetiedostot pyydämme tarvittaessa erikseen vastaanotettuamme raportin.
- Saatamme hyödyntää tai julkaista korjattujen havaintojen osalta koostettuja ja

toimitettuja yhteenvetoja joista on poistettu kaikki mahdolliset yksityiset ja henkilökohtaiset tiedot. Pyrimme tekemään mahdollisen havainnon julkaisun yhteisymmärryksessä raportoijan kanssa. Emme jaa tietoja duplikaateista joita ei ole vielä julkaistu.

RAPORTIN SISÄLTÖ

Raportoijalle on tarjolla tähän ohjelmaan soveltuvat raportointipohjat. Niiden käyttö on vapaaehtoista, mutta suotavaa.

Raportissa ilmoitettu haavoittuvuus pitää pystyä todentamaan. Jos emme voi todentaa ilmoitusta toistamalla, emme voi myöskään palkita ko. havainnosta. Internet-selaimen toimintaan liittyvät haavoittuvuudet on pystyttävä toistamaan modernilla (HTML5-yhteensopivalla) Internet-selaimella.

Seuraavista asioista lähetettyjä raportteja emme välttämättä hyväksy osaksi ohjelmaa:

- Automaattiskannereiden (useasti erittäin spekulatiiviset ja epätarkat) tulokset
- Sähköpostipalvelimiin liittyviä konfiguraatioita (SPF, DMARC, ...)
- SSL/TLS konfiguraatioiden parhaita käytäntöjä tai niiden puutteita (ellei havaintoon liity selkeästi hyväksikäytettävissä olevaa uhkaa tai heikkoutta)
- SSL/TLS konfiguraatioihin liittyviä yksittäisiä CVE-havaintoja tai havaintoja jotka on löydettävissä SSLabs-skannerilla (tai vastaavalla)
- HTTP security headereihin liittyviä parhaita käytäntöjä tai niiden puutteita
- Lomakkeita, joissa on teoreettinen CSRF-haavoittuvuus (ilman toimivaa PoCia joissa osoitetaan uhka ja sen toteuttaminen)
- Logout CSRF -havaintoja
- Salasanapolitiikkoihin tai salasanojen vahvuuteen liittyviä havaintoja
- Web-sisällön injektointia (engl. content spoofing / text injection)
- Palvelun teknisestä alustasta vuotavia versionumero yms. tietoja, joihin ei liity selkeästi osoitettavissa ja hyväksikäytettävissä olevaa uhkaa tai heikkoutta.
- Evästekonfiguraatioihin liittyviä havaintoja
- Virhesivukonfiguraatioihin liittyviä havaintoja
- XSS johon ei liity mitään osoitettua uhkaa tai heikkoutta
- Havaintoja puutteista, haavoittuvuuksista tai ongelmista, jotka eivät ole suoranaisesti Verohallinnon vaikutuspiirissä.

JULKAISUKIELTO JA MUUTA HUOMIOITAVAA

Lähettäessään raportin raportoija sitoutuu julkaisukieltoon liittyen raportin sisältämään haavoittuvuuteen. Haavoittuvuudesta ei saa antaa tietoa kolmansille osapuolille. Palkintoa ei makseta, jos jokin kolmas osapuoli saa tiedon raportoidusta haavoittuvuudesta.

Verohallinto voi halutessaan erikseen kirjallisesti antaa luvan haavoittuvuustietojen julkaisuun.

Raportoijan niin halutessa voimme julkistaa nimen tai nimimerkin mahdollisella kiitos-sivulla tai top-listauksessa.

Jos useampi henkilö raportoi saman haavoittuvuuden, lähtökohtaisesti vain ensimmäinen raportoija saa palkinnon. Myöhemmille raportoijille kerrotaan, että haavoittuvuus on jo käsitelty.

PALKINNOT

Ohjelman suurin palkinto on 30.000€ ja pienin palkinto on 100€. Palkinnot maksetaan työkorvauksena ja sen edellytyksenä on verokortin ja tilinumeron toimittaminen Hackrfi Oy:lle palkkion maksua varten. Ilman suomalaista verokorttia ja tilinumeroa palkintoa ei voi maksaa. Palkinnon maksajana toimii Hackrfi Oy.

Suurimman palkinnon saa esimerkiksi tilanteessa, jossa löytää haavoittuvuuden tai haavoittuvuuksien ketjun, jossa saa käsiinsä merkittävän määrän OmaVero-palvelussa säilytettävien ihmisten henkilö- tai verotustietoja.

Sovellamme riski- ja impaktipohjaista arviointia palkkioissamme. Arvioimme havainnot pääasiallisesti haavoittuvuuden mahdollisen seurauksen näkökulmasta. Jos raportoitu haavoittuvuus ei tulkintamme mukaan muodosta riskiä tai ei ole tietoturvahaavoittuvuus, pidätämme oikeuden olla palkitsematta ko. havainnosta. Palkintoa ei makseta jos käy ilmi, että haavoittuvuus on löydetty sääntöjen vastaisilla keinoilla.

Pyrimme olemaan perusteluissamme avoimia ja läpinäkyviä ja perustelemalla päätöksiämme raportoijalle. Jos yhdestä bugista on monta ilmentymää, esimerkiksi ongelma jaetussa kirjastossa, voidaan raportit ja palkkiot yhdistää. Yleisesti käytössä olevista ja julkisesti saatavilla olevista kirjastoista löytyneistä haavoittuvuuksista saatamme maksaa normaalia pienemmän korvauksen.

Jos löydetty haavoittuvuus on Verohallinnon palvelun ja sille palveluita tarjoavan tahon (esim. Väestörekisterikeskus) välisessä rajapinnassa, ja tällä taholla on oma Hackrfi Oy:n haavoittuvuuspalkkio-ohjelmansa, palkkio voidaan siirtää maksettavaksi palveluntarjoajan haavoittuvuuspalkkio-ohjelmasta. Vastaavasti tästä Verohallinnon ohjelmasta voidaan maksaa haavoittuvuuspalkkioita haavoittuvuuksista, jotka on alun perin raportoitu palveluntarjoajan ohjelmaan. Tällaiset siirrot tehdään aina yhteisymmärryksessä Verohallinnon ja palveluntarjoajan kanssa. Maksun siirron tarkoitus ei ole minimoida maksettavaa summaa, vaan löytää maksajaksi organisaatio, joka on vastuussa

haavoittuvasta osiosta.

OIKEUDELLISET LISÄVAATIMUKSET

Raportoimalla haavoittuvuudesta Hackrfi Oy:lle raportoija myöntää Hackrfi Oy:lle ja Verohallinnolle kaikki oikeudet raportin sisältämiin tietoihin ja niiden hyödyntämiseen löydöksen korjaamiseksi.

Verohallinto (eli Tilaaja) myöntää tähän ohjelmaan osallistuville tietoturvatestaajille oikeuden toteuttaa Tilaajan järjestelmään haavoittuvuustestaustoimia ja -toimenpiteitä, jotka voitaisiin tulkita tietomurron tai tietoliikenteen häiritsemisen yritykseksi. Tilaaja sitoutuu olemaan tekemättä Ohjelman sääntöjen mukaisesti tehdyistä tietoturvatestaajien haavoittuvuustestaustoimista ja -toimenpiteistä tutkintapyyntöjä rikoslain (19.12.1889/39) 38. luvun 5§, 6§ tai 7§:ien tarkoittamissa tapauksissa ja olemaan vaatimatta niistä rikosoikeudellisia seuraamuksia.

Epäselvissä tilanteissa tietoturvatestaaja on velvollinen pyytämään Ohjelman järjestäjän Hackfri Oy:n ja Tilaajan lupaa tietyn toimenpiteen toteuttamiseksi. Annettu lupa sitoo Järjestäjää ja Tilaajaa. Tietoturvatestaajaa sitoo hänen antamansa toimenpidesuunnitelma. Mikäli Ohjelman Järjestäjä tai Tilaaja antaa ohjeistusta tai täydentää tietoturvatestaajan toimenpidesuunnitelmaa, sitovat annetut ohjeet sekä tietoturvatestaajaa että Järjestäjää ja Tilaajaa.

Tietoturvatestaajien oikeus testata Tilaajan järjestelmää päättyy viimeistään Ohjelman päättyessä.

Tietoturvatestaaja on tietoinen ja hyväksyy sen, että Ohjelman sääntöjen vastainen toiminta voi johtaa rikosoikeudellisiin seuraamuksiin. Ohjelman Tilaaja pidättää oikeuden tehdä Ohjelman sääntöjen vastaisesta toiminnasta tutkintapyynnön Poliisille. Lisäksi Tilaaja pidättää oikeuden vaatia asiassa rangaistusta ja/tai vahingonkorvausta.