HAAVOITTUVUUSPALKKIO-OHJELMAN SÄÄNNÖT JA EHDOT

Näitä sääntöjä ja ehtoja sovelletaan Digi- ja väestötietoviraston (DVV) haavoittuvuuspalkkio-ohjelmaan, jonka järjestäjänä on Hackrfi Oy.

Tässä ohjelmassa tarkoituksena on havaita kriittisiä tietoturvahaavoittuvuuksia DVV:n palveluissa (katso tarkemmin kohdasta ohjelman laajuus) noudattaen tässä dokumentissa olevia sääntöjä ja ehtoja. 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 palkkioita 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 haavoittuvuuspalkkio-ohjelmaan osallistuminen ja siihen liittyvän tietoturvatutkimuksen suorittaminen ei aiheuta ennalta arvaamattomia tietoturvariskejä Digi- ja väestötietoviraston asiakkaille tai asiakastiedoille.

OHJELMAN LAAJUUS

Kohteet ovat

- Suomi.fi-verkkopalvelu palvelimineen mukaan lukien palvelun tunnistusratkaisun (Suomi.fi-tunnistus) sekä valtuuksien (suomi.fi-valtuudet) rajapinnat osoitteessa: https://www.suomi.fi/
- Seuraavat varmennepalveluihin liittyvät kohteet:
  - Tukevat palvelut https://dvv.fineid.fi/
  - Varmennekortin uusinnan Itsepalveluportaali https://haevarmenne.vrk.fi/
  - DigiSign-kortinlukijaohjelmisto, jonka voit hakea osoitteesta https://dvv.fi/kortinlukijaohjelmisto (Win/Linux/Mac). Tämä kohde on työasemaohjelmisto.
- Seuraavat väestötietojärjestelmän kyselypalvelut
  - https://vtjkyselykoulutus.2016.vrk.fi/
  - Rajapintapalvelu https://vtjkyselykoulutus.2016.vrk.fi/sosowebsiteIP/soso.asmx
  - https://vrkkayttajapalvelut.2016.vrk.fi/salasanantilaus/

Lisärajaukset:

- Rekistereistä mukaan otetaan vain DVV:n ”Henkilötiedot”. Muiden virastojen rekisterit rajataan tästä ohjelmasta pois.
- Suomi.fi-tunnistuksen ulkopuoliset tunnistuspalvelut, esimerkiksi pankkien tunnistuspalvelut, ovat mukana vain DVV-integraation osalta. Niitä käyttäen saa siis tunnistautua testatakseen esim. Henkilötiedot-rekisteriä, tai sitä miten tiedot ulkopuoliselta palveluntarjoajalta välitetään DVV:lle, mutta itse ulkopuolista tunnistuspalvelua ei saa testata.
- Suomi.fi-tunnistus hyödyntää tunnistuksen välityspalvelua (palveluntarjoajana OP). Välityspalvelun osalta mahdolliset huomiot voi raportoida siinä määrin kun ne tulevat esiin Suomi.fi-tunnistuksen kautta tunnistauduttaessa.
- Palautelomakkeet on rajattu ohjelman ulkopuolelle.
- Keväällä 2024 on presidentinvaalit, joiden aikana ei saa tehdä testausta. Nämä vaalirauhapäivät ilmoitetaan myöhemmin.

Mistä olemme erityisesti kiinnostuneita: Asiakkaiden henkilötietojen oikeudeton paljastuminen, toisen henkilön identiteetin hyödyntäminen sekä käyttäjien oikeuksien laajentaminen tai valtuuksien väärinkäyttö.

Muut DVV:n palvelut eivät ole tämän ohjelman piirissä.

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**: Haavoittuvuuspalkkio-ohjelmaan osallistuja ei saa olla osallistunut nyt käytössä olevien Suomi.fi-palvelujen suunnitteluun, toteutukseen tai testaamiseen eikä sen tietoturvatarkastuksen tekemiseen viimeisen kahden vuoden aikana.
- **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.
- **Toiminnan 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 haavoittuvuuspalkkio-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” ja muut DVV:n tai sen alihankkijoiden työntekijöihin kohdennetut hyökkäykset.
- Fyysisen tason hyökkäykset, esim. MitM-hyökkäykset.
- Yksilön turvallisuuden uhkaaminen.
- 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.
- Kohdejärjestelmän tietojen ohjaaminen niiden fyysisen käyttöympäristön ulkopuolelle esim. hyökkääjän järjestelmään.

HAAVOITTUVUUDEN RAPORTOINTI

Havaittu haavoittuvuus on raportoitava osoitteeseen https://www.hackr.fi linkatun raportointiportaalin ohjelmakohtaisen lomakkeen 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 10 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.
- Kuva- ja PDF-liitteet voi liittää raporttiin, muiden liitetiedostojen (esim. videot) toimituksesta sovitaan erikseen. Mainitse kuitenkin, jos sinulla on tällaista tukimateriaalia.
- 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

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 Digi- ja väestötietoviraston vaikutuspiirissä.

JULKAISUKIELTO JA MUUTA HUOMIOITAVAA

Lähettäessään raportin raportoija sitoutuu julkaisukieltoon liittyen raportin sisältämään haavoittuvuuteen. Haavoittuvuudesta ei saa antaa tietoa kolmansille osapuolille. Palkkiota ei makseta, jos jokin kolmas osapuoli saa tiedon raportoidusta haavoittuvuudesta. Digi- ja väestötietovirasto voi halutessaan erikseen kirjallisesti antaa luvan haavoittuvuustietojen julkaisuun.

Jos Digi- ja väestötietovirasto on päättänyt maksaa havainnoitsijalle palkkion, palkkionmaksupäätös on julkinen.

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 palkkion. Myöhemmille raportoijille kerrotaan, että haavoittuvuus on jo käsitelty.

PALKKIOT

Ohjelman suurin palkkio on 30 000€ ja pienin palkkio on 100€. Palkkiot maksetaan työkorvauksena ja sen edellytyksenä on verokortin ja tilinumeron toimittaminen Hackrfi Oy:lle palkkion maksua varten. Ilman suomalaista verokorttia ja tilinumeroa palkkiota ei voi maksaa. Palkkion maksajana toimii Hackrfi Oy.

Suurimman palkkion saa esimerkiksi tilanteessa, jossa löytää haavoittuvuuden tai haavoittuvuuksien ketjun, jota hyödyntämällä voi saada tietoonsa merkittävän määrän palvelua käyttävien ihmisten henkilötietoja.

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. Palkkiota 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 Digi- ja väestötietoviraston palvelun ja sen palveluita hyödyntävän tahon välisessä rajapinnassa, ja tällä taholla on oma haavoittuvuuspalkkio-ohjelmansa, palkkio voidaan siirtää maksettavaksi hyödyntävän tahon mahdollisesta haavoittuvuuspalkkio-ohjelmasta. Vastaavasti tästä DVV:n ohjelmasta voidaan maksaa haavoittuvuuspalkkioita haavoittuvuuksista, jotka on alun perin raportoitu DVV:n palveluita hyödyntävän tahon ohjelmaan. Tällaiset siirrot tehdään aina yhteisymmärryksessä Digi- ja väestötietoviraston sekä hyödyntävän tahon 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 sekä Digi- ja väestötietovirastolle kaikki oikeudet raportin sisältämiin tietoihin ja niiden hyödyntämiseen löydöksen korjaamiseksi.

Digi- ja väestötietovirasto (eli Tilaaja) myöntää tähän ohjelmaan osallistuville tietoturvatestaajille oikeuden toteuttaa Tilaajan tämän ohjelman kohdejärjestelmään 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§:n tarkoittamissa tapauksissa ja olemaan vaatimatta niistä rikosoikeudellisia seuraamuksia.

Tietoturvatestaajien oikeus testata Tilaajan järjestelmää päättyy viimeistään Ohjelman päättyessä.

Epäselvissä tilanteissa tietoturvatestaaja on velvollinen pyytämään Ohjelman järjestäjän Hackrfi Oy:n ja Tilaajan lupaa tietyn toimenpiteen toteuttamiseksi.