HAAVOITTUVUUKSIEN KOORDINOINTIPOLITIIKKA

v1.1

2012-06-15

Johdanto

CERT-FI on kansallinen tietoturvaviranomainen, jonka tehtävänä on edistää turvallisuutta tietoyhteiskunnassa ennaltaehkäisemällä, valvomalla ja selvittämällä tietoturvaloukkauksia sekä tiedottamalla tietoturvauhista.

CERT-FI:n näkemyksen mukaan ohjelmistohaavoittuvuudet ovat vakava uhka tietoyhteiskunnan normaalille toiminnalle. On itsestään selvää, että haavoittuvuudet täytyy ensin tunnistaa, ennen kuin niitä voidaan tyydyttävästi korjata tai niiden aiheuttama uhka voidaan muulla tavoin poistaa. Lisäksi on havaittu, että ohjelmistojen testausmenetelmien käyttö ja tietoturvatutkimuksen näkökulmien hyödyntäminen voivat auttaa ennestään tuntemattomien haavoittuvuuksien tunnistamisessa. Löydöksiä täytyy kuitenkin käsitellä vastuullisesti, koska niillä voi olla kauaskantoisia haittavaikutuksia ihmisten yksityisyyteen, omaisuuteen ja liiketoimintaan, ja jopa kansalliseen turvallisuuteen.

Haavoittuvuuskoordinoijana CERT-FI edistää haavoittuvuustietojen vastuullista käsittelyä haavoittuvuuden elinkaaren kaikissa vaiheissa, ei ainoastaan haavoittuvuuden paljastumisen aikaan. Haavoittuvuuden tunnistaminen ei yksin riitä. Haavoittuvuuden aiheuttamat haitat täytyy korjata, korjaukset täytyy saattaa käyttäjien ulottuville ja korjaukset täytyy myös saada käyttöön, jotta niistä olisi hyötyä. Koordinoijien tavoitteena on löytää tasapaino haavoittuvuuksien löytäjien, ohjelmistovalmistajien, ohjelmistointegraattoreiden ja loppukäyttäjien etujen välillä. Tähän pyritään varmistamalla, että mahdollisimman monet merkittävät haavoittuvuudet korjataan ja korjaukset otetaan käyttöön.

Tavoitteet

CERT-FI:n tavoite on vähentää ohjelmistohaavoittuvuuksien haittavaikutuksia tai poistaa ne täysin. Tämä tavoite saavutetaan tarjoamalla haavoittuvuuskoordinointipalveluja useiden tahojen hyödyksi, etenkin haavoittuvuuksien löytäjien, ohjelmistovalmistajien, ohjelmistointegraattoreiden ja loppukäyttäjien hyväksi. Suuren yleisön oikeus tietää tietoturvahaavoittuvuuksista täytyy tasapainottaa ohjelmistovalmistajien prosessien ja liiketoiminnan tarpeiden kanssa. Lisäksi tulee ottaa huomioon niiden loppukäyttäjien tietoturvatarpeet, joita haavoittuvuus koskee. CERT-FI pyrkii toimimaan luotettuna välittäjänä haavoittuvuuksien löytäjien, haavoittuvuuden vaikutuspiiriissä olevien ohjelmistovalmistajien ja suuren yleisön välillä.

Haavoittuvuuskoordinoinnin aloittaminen

Koordinointiprosessi alkaa yleensä siten, että haavoittuvuuden alkuperäinen löytäjä (myöhemmin Raportoija) raportoi haavoittuvuudesta CERT-FI:lle pyytäen apua ohjelmistovalmistajien tavoittamisessa tai asiasta tiedottamisessa niille tahoille, joihin haavoittuvuus vaikuttaa. CERT-FI pyrkii vastaamaan raporttiin seitsemän arkipäivän kuluessa. Ennen kuin CERT-FI ottaa vastuulleen uuden haavoittuvuuskoordinointiprojektin, kahden ehdon tulee täyttyä.

1. Raportoijan ja CERT-FI:n tulee päästä yhteisymmärrykseen projektista ja sen tavoitteista.

    - Myös yksityiskohdista täytyy päästä sopimukseen; esimerkiksi projektin vaiheista ja haavoittuvuuteen liittyvien, mahdollisesti arkaluontoistenyksityiskohtien hoitamisesta ennen haavoittuvuuden julki tuomista täytyy sopia.
    - Haavoittuvuuden julkistamisen laajuudesta tulee myös päästä yhteisymmärrykseen. Yhteinen näkemys projektin toivotusta lopputuloksesta on osoittautunut ensiarvoisen tärkeäksi projektin onnistumisen kannalta.

2. Haavoittuvuuslöydöksen tulee olla tarpeeksi merkittävä, jotta CERT-FI:n kannattaa panostaa siihen koordinointityötä.

    - Koordinointiprojekteja priorisoidaan haavoittuvuuden arvioidun vaikutuksen, senhetkisen uhkatilanteen ja CERT-FI:n resurssien mukaan.
    - Koordinoinnissa priorisoidaan haavoittuvuuksia, jotka vaikuttavat moneen ohjelmistovalmistajaan ja useisiin tuotteisiin.
    - Jos haavoittuvuus vaikuttaa laajaan käyttäjäkuntaan tai tärkeisiin infrastruktuureihin ja CERT-FI:n koordinointityön katsotaan tuovan lisäarvoa tilanteen selvittämiseen,

CERT-FI useimmiten hyväksyy projektin vastuulleen.
- Sen sijaan vähäpätöiset tai vain harvoja käyttäjiä tai toteutuksia koskettavat haavoittuvuudet saatetaan jättää hyväksymättä.
- CERT-FI voi auttaa Raportoijaa löytämään asianmukaiset tietoturvayhteyshenkilöt, vaikka muuta koordinointityötä ei aloitettaisi.

CERT-FI käyttää haavoittuvuuksiin liittyvässä viestinnässä sähköpostiosoitetta vulncoord@ficora.fi. PGP-avaimet sähköpostiosoitteelle löytyvät sivulta https://www.cert.fi/en/activities/contact/pgp-keys.html.

Julkistamisaikataulu

CERT-FI:n tietoon saatettujen haavoittuvuuksien julkistamisaikataulusta neuvotellaan mahdollisuuksien mukaan niiden ohjelmistovalmistajien kanssa, joihin haavoittuvuus vaikuttaa. Jos ohjelmistovalmistajaa ei tavoiteta tai julkistamisaikatauluista ei päästä yhteisymmärrykseen, tieto haavoittuvuudesta voidaan julkistaa 42 päivää ensimmäisen raportin jälkeen, riippumatta siitä onko korjauksia tai rajoitusmenetelmiä olemassa tai saatavilla. Pääasiallinen julkistamiskanava ovat CERT-FI:n kotisivuilla julkaistut tietoturvatiedotteet.

Lopullinen julkistamisaikataulu päätetään kuitenkin tapauskohtaisesti. Olosuhteiden muutokset, kuten haavoittuvuuden aktiivinen hyväksikäyttö, erityisen vakavat uhat, tai vakiintuneisiin standardeihin muutoksia vaativat tilanteet voivat johtaa aikataulun muutoksiin.

Yhteydenotot ohjelmistovalmistajiin

Haavoittuvuusraportin saatuaan CERT-FI pyrkii kertomaan haavoittuvuuden yksityiskohdista haavoittuvuuden vaikutuspiirissä oleville ohjelmistovalmistajille niin pian kuin se on käytännön kannalta järkevää. CERT-FI koettaa löytää sopivan yhteyshenkilön ohjelmistovalmistajan taholta, alkaen valmistajan antamista tuoteturvallisuusyhteystiedoista. Valmistajille annetaan viisi päivää aikaa vastata ensimmäiseen yhteydenottoon. CERT-FI varaa oikeuden julkistaa haavoittuvuustiedotteissaan listan ohjelmistovalmistajista, joita se on koettanut tavoittaa kyseisen haavoittuvuuden kohdalla.

Jos ohjelmistovalmistajaan ei saada yhteyttä, valmistaja voi jäädä tulevan tiedonkulun ulkopuolelle. Haavoittuvuuteen liittyvien yksityiskohtien julkistamista saatetaan nopeuttaa, jos ohjelmistovalmistajan reagoimattomuudesta katsotaan aiheutuvan tietoturvauhkaa loppukäyttäjille.

CERT-FI varaa oikeuden käyttää luotettuja kolmansia osapuolia, kuten muita koordinoijia ja CSIRT-ryhmiä, apuna haavoittuvuustietojen välittämisessä ohjelmistovalmistajille. CERT-FI voi myös varoittaa luotettuja kolmansia osapuolia ennen haavoittuvuustiedon julkaisemista. Ohjelmistovalmistajille tiedotetaan tiedon saaneista muista osapuolista mahdollisuuksien mukaan.

Haavoittuvuusyksityiskohdat ja yhteydenpito ohjelmistovalmistajiin salataan PGP:n tai S/MIME:n avulla arkaluontoisten tietojen turvaamiseksi aina kun se on mahdollista.

Haavoittuvuuksien käsittelyn standardit

CERT-FI varmistaa CVE-numeroiden hankkimisen haavoittuvuuksille, jotka se hyväksyy koordinoinnin kohteeksi.

Kreditointi

Pääsääntöisesti CERT-FI kreditoi Raportoijaa, ellei toisin ole toivottu.

Hyväksikäyttöesimerkkien ja analyysien tarjonta

CERT-FI ei julkaise esimerkkejä haavoittuvuuksien hyväksikäyttämisestä edes esittelytarkoituksissa. Resurssirajoitusten vuoksi syvällisiä haavoittuvuusanalyysejä tehdään vain, jos tärkeä yhteistyökumppani sellaista toivoo tai jos kyseisen haavoittuvuuden vaikutukset ovat merkittävät.

Oikeudellinen huomautus

Suomen velvoittava lainsäädäntö, erityisesti Laki viranomaisten toiminnan julkisuudesta (621/1999), voi joissain tapauksissa asettaa reunaehtoja haavoittuvuustietojen prosessoimiselle ja julkistamiselle.

CERT-FI:n tehtäväksi on lailla määrätty kerätä tietoja tietoturvauhkista julkisissa viestintäverkoissa ja palveluissa, sekä tutkia kyseisiä uhkia. CERT-FI:n velvollisuudet on kuvattu Sähköisen viestinnän tietosuojalain (516/2004) pykälässä 31.

Määritelmiä

Haavoittuvuus alttius turvallisuutta uhkaaville tekijöille, puutteet ja heikkoudet turvatoimissa sekä suojauksissa.[1]

Hyväksikäyttömenetelmä (engl. exploit) Arkikielessä "exploit script" (hyväksikäyttöskripti): skripti/komentosarja, ohjelma, mekanismi tai muu tekniikka, jonka avulla haavoittuvuutta hyväksikäytetään tietovarmuuteen liittyvän tavoitteen saavuttamiseksi. Alalla käytetään yleisesti termejä "hyväksikäyttää" ja "exploit script", kun viitataan muihinkin kuin skripteihin/komentosarjoihin, jotka hyödyntävät haavoittuvuuksia.[2]

CSIRT CSIRT-toiminnalla tarkoitetaan tietoturvaloukkauksien ennaltaehkäisyä, niiden havainnointia ja ratkaisua sekä tietoturvauhkista tiedottamista. CSIRT-organisaatioita on useita ympäri maailmaa. CSIRT-organisaatiot toimivat yhteistyössä keskenään jakaen tietoa tietoturvaloukkauksista ja niihin liittyvistä seikoista sekä tiedottavat niistä järjestelmien käyttäjille esimerkiksi Internetin välityksellä. CSIRT-toiminnan päämääränä on tietojärjestelmien tietoihin kohdistuvien tietoturvaloukkauksien ja uhkien toteutumisen ennaltaehkäisy ja torjunta mahdollisimman objektiivisesti ja tehokkaasti.

Lisäaineistoa

Tämä toimintapolitiikka on laadittu CERT/CC:tä mukaillen yhteistyössä kyseisen tahon kanssa. CERT/CC:n haavoittuvuuksien julkistamispolitiikka on saatavilla osoitteessa:

http://www.kb.cert.org/vuls/html/disclosure

Kokoelma muita haavoittuvuuksien julkistamispolitiikkoja ja ohjeita on saatavilla Oulun yliopiston University Secure Programming Groupin (OUSPG) kotisivuilla.[3]

---

[1] Valtionhallinnon tietoturvasanasto VAHTI 8/2008, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/name.jsp

[2] Käännetty suomeksi Viestintävirastossa Carnegie Mellonin määritelmästä: Carnegie Mellon, Software Engineering Institute, State of the Practice of Intrusion Detection Technologies, http://www.sei.cmu.edu/reports/99tr028.pdf

[3] OUSPG, Disclosure policies and Guidelines, https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking#Disclosure_policies_and_Guidelines