STATE OF SOFTWARE SECURITY

KATSAUS SOVELLUSTEN JA SOVELLUSKEHITYKSEN TIETOTURVAN TILAAN

NRO 9

VERACODE

Yhteenveto

Veracoden julkaisemassa yhdeksännessä State of Software Security (SOSS), Katsaus sovellusten ja sovelluskehityksen tietoturvan tilaan -raportissa esitetyt tunnusluvut muodostavat alan kattavimmat sovellusten tietoturvatason arviointikriteerit. Analyysimme pohjana olevat tiedot on kerätty skannaamalla todellisia, käytössä olevia sovelluksia Veracode App Sec -ohjelman asiakastestauksen yhteydessä. Se kattaa yli 2 biljoonaa koodiriviä, jotka ovat peräisin 700 000 skannatusta sovelluksesta 12 kuukauden ajalta 1.4.2017 – 31.3.2018.

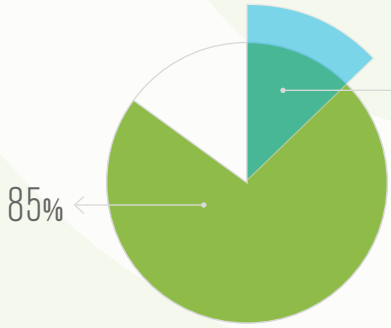
Raportin aiempien versioiden tapaan annamme tarkan kuvan siitä, kuinka hyvin sovelluksissa noudatetaan alan parhaita käytäntöjä, kuten OWASP Top 10, ja millaisia haavoittuvuuksia tyypillisissä sovelluksissa useimmin esiinty:

PARHAIDEN KÄYTÄNTÖJEN NOUDATTAMINEN

OWASP Top 10:
n noudattamis-aste laski kolmatta vuotta peräkkäin, nyt

22.5%

Yli 85 prosentissa sovelluksista on ainakin yksi haavoittuvuus ja yli 13 %:ssa ainakin yksi kriittinen tietoturvariski.



Korjausasteet paranivat 12 prosenttiyksiköllä tänä vuonna – **asiakkaat paikkasivat lähes**

70%

löydetyistä haavoittuvuuksista

Ohjelmistoissa on edelleenrunsaasti haavoittuvia komponentteja.

NOIN


87.5% Java

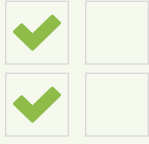

92% C++


85.7% .NET

-sovelluksista sisältää ainakin yhden haavoittuvan komponentin.

YLEISIMMÄT SOVELLUKSISSA ESIINTYVÄT HAAVOITTUVUUDET PYSYIVÄT SUURELTA OSIN SAMOINA:

SQL-injektio-haavoittuvuuksia esiintyy edelleen lähes joka kolmannessa sovelluksessa.



Sivustojen välisten komentosarjojen (XSS) haavoittuvuuksia on lähes 50 %:ssa sovelluksista.

Raportin laatimisen yhteydessä havaitsimme, että keräämämme data voisi antaa vielä syvällisempää tietoa kuin vakiotunnusluvut, joita olemme aiemmin analysoineet.

Sovellusten tietoturvaohjelman tärkein mittari on, miten tehokkaasti haavoittuvuudet korjataan niiden havaitsemisen jälkeen. Tavoitteenamme oli tänä vuonna syventää tilastoja, jotka kertovat kauanko eri tyyppisten haavoittuvuuksien paikkaaminen kestää, sekä ymmärtää, miksi tietyt riskit jäävät elämään niin pitkäksi aikaa kuin nyt tapahtuu

HAAVOITTUVUUKSIEN KORJAAMINEN

Cyentia-instituutin datatutkijat auttoivat meitä kokoamaan tiedot haavoittuvuuksien korjaamisesta käytännön tasolla. Pystyimme erittelemään, miten eri tekijät, kuten virhetyyppi, sovelluksen kriittisyys ja skannaustiheys vaikuttavat korjausnopeuteen ja toisaalta virheiden pysyvyyteen niiden havaitsemisen jälkeen:

- Kuukauden kuluttua löytymisestä yli 70 % virheistä oli edelleen olemassa ja vielä 3 kuukauden kuluttua lähes 55 %.
- Joka neljäs vakavaksi ja erittäin vakavaksi luokiteltava tietoturvapuute on edelleen korjaamatta 290 päivän kuluttua löytymisen jälkeen
- Sovelluksissa, jotka skannataan vain 1–3 kertaa vuodessa, virheet pysyvät 3,5 kertaa pidempään kuin niissä, joita testataan 7–12 kertaa vuodessa.
- DevSecOps-yksisarvisia on olemassa ja ne korjaavat viat huomattavasti verrokkeja tehokkaammin.
- Suurimmissa vaikeuksissa havaittujen vikojen korjaamisessa ovat infrastruktuuri-, teollisuus- ja rahoitusala.

Tietojen analysointi antaa tietoturva-alan ammattilaisille ja kehitystiimeille tärkeää tietoa siitä, miten he voivat saavuttaa mitattavissa olevaa edistystä sovellusriskien vähentämisessä. Toivomme, että lukijamme pystyvät hyödyntämään näitä vertailuarvoja tehokkaasti

Lue koko raportti

veracode.com/soss

TIETOJA VERACODESTA

Veracode auttaa organisaatioita varmistamaan niiden toimintaan olennaisesti liittyvien ohjelmistojen tietoturvallisuuden ja on alansa johtava toimija. Veracoden SaaS-alusta ja integroidut ratkaisut auttavat tietoturvatiimejä ja sovelluskehittäjiä löytämään ja korjaamaan tietoturvaongelmat kaikissa sovelluskehityksen vaiheissa jo ennen kuin ne altistuvat tietomurroille. Kattava tarjontamme auttaa asiakkaita vähentämään tietomurtojen riskiä, nopeuttamaan sovelluskehitystä turvallisesti, täyttämään normien vaatimukset sekä turvaamaan ohjelmistovarallisuutensa kustannustehokkaasti – olipa kyse ohjelmistojen kehittämisestä, ostamisesta tai myymisestä.

Veracode palvelee yli 1400 asiakasta monilla eri toimialoilla, mukaan lukien lähes kolmasosa Fortune 100 -yrityksistä, kolme neljästä yhdysvaltalaisesta suurpankista ja yli 20 Forbesin listaamista 100:sta arvokkaimmasta brändistä. Lue lisää osoitteesta **www.veracode.com, Veracoden blogista, Twitteristä ja Veracode-yhteisöstä.**