Sadržaj

Klasifikacija sigurnosnih napada

U nastavku je dan primjer klasifikacije sigurnosnih napada korištenjem predložene taksonomije četiri pogleda.

SQL SLammer

Svrha napada

- Korupcija podataka – crv unosi lažne podatke u bazu ili mijenja postojeće
- Uskračivanje usluge (engl. Denial-of-service) – crv se pokušava širiti na druge poslužitelje čime koristi velike količine računalnih resursa što dovodi do zagušavanja

Meta napada

- SQL server baza podataka

Metoda napada

- Iskorištavanje slabosti

Ranjivost koja se iskorištava

- Preljev spremnika – ranjivost u bazi podataka MS SQL 2000 omogućuje izvršavanje proizvoljnih naredbi sa povećanim privilegijama. Konkretna ranjivost http://www.kb.cert.org/vuls/id/484891

HD Audio Codec Driver

Svrha napada

- Povećanje pristupa – izvršavanjem napada napadač dobiva administrativne privilegije na Windows računalu, odnosno SYSTEM privilegije. Napadač može čitati, pisati i stvarati proizvoljne vrijednosti u registry sustava.

Meta napada

- Računalo – iskorištavanjem ranjivosti moguće je izvršavati proiizvoljne naredbe na žrtvi.

Metoda napada

- Iskorištavanje slabosti – neispravno filtriranje ulaznih parametara uzrokuje preljev spremnika.

Ranjivost koja se iskorištava

- Preljev spremnika – datoteke RTKVHDA.sys i RTKVHDA64.sys neispravno validiraju IOCTL zahtjev koji rezultira preljevom spremnika. Prilagođenim zahtjevom napadač može izvršavati proizvoljne naredbe na žrtvi.

Windows 'AFD.sys' Driver

Svrha napada

- Uskraćivanje usluge – iskorištavanjem ranjivosti ciljano računalo prestaje reagirati na daljnje naredbe korisnika, čime se postiže uskraćivanje usluge.

Meta napada

- Računalo – žrtve su računala koja koriste Microsoft Windows XP operacijski sustav sa programskim dodatkom SP3. Napad je ograničen na jedno računalo.

Metoda napada

- Iskorištavanje slabosti – izvršavanje posebno stvorenog IOCTL zahtjeva na računalu žrtvi.

Ranjivost koja se iskorištava

- Greška u dizajnu – neispravnim rukovanjem IOCTL zahtjevima pristupa se neispravnoj memorijskoj lokaciji što uzrokuje grešku sustavu od koje se nije moguće oporaviti.

Ruby on Rails limit() funkcija

Svrha napada

- Korupcija informacija – izvođenjem proizvoljnih upita nad bazom podataka napadač mijenja sadržaj i time narušava ispravnost podataka.
- Narušavanje tajnosti – napadač dobiva pristup svim podacima čime se narušava tajnost.

Meta napada

- Baza podataka – naredbe se prosljeđuju prema pozadinskoj bazi podataka što omogućuje napadaču izravan pristup podacima. Ovisno o svrsi napada, napadač će obavljati izmjenu podataka (što u nekim situacijama može u potpunosti onesposobiti web sjedište) ili izlistavati određene stavke čime se narušava tajnost.

Metoda napada

- Iskorištavanje slabosti – iskorištavanjem neispravnog filtriranja SQL naredbi napadač može izvršavati proizvoljne naredbe nad bazom podataka bez prethodne autentifikacije.

Ranjivost koja se iskorištava

- Greška u dizajnu – neispravno filtriranje korisničkog unosa. Korisnički unos se prosljeđuje do jezičnog prevoditelja baze podataka koji će prevesti i izvršiti naredbe koje su predane kao korisnički unos.

OpenVAS Manager

Svrha napada

- Povećanje pristupa – OpenVas Manager neispravno filtrira korisnički unos što omogućuje izvršavanje proizvoljnih naredbi sa povećanim privilegijama.

Meta napada

- Računalo – žrtve su računala koja koriste OpenVas Manager i GSA web aplikaciju.

Metoda napada

- Iskorištavanje slabosti – iskorištavanjem neispravnog filtriranja unosa napadač dobiva povećane ovlasti za izvršavanje naredbi na računalu žrtvi.

Ranjivost koja se iskorištava

- Greška u dizajnu – neispravno filtriranje korisničkog unosa prilikom obrade OMP zahtjeva poslanih od strane autoriziranih korisnika GSA (engl. Greenbone Security Assistant) web aplikacije. Ranjivost se može iskoristiti za izvođenje proizvoljnih naredbi sa ovlastima OpenVas Manager računa (obično root).

BlackBerry Desktop programska potpora

Svrha napada

- Narušavanje tajnosti – napadač želi pristupiti informacijama pohranjenim na uređaju.

Meta napada

- Uređaj – meta napada su podaci koje se nalaze na uređaju BlackBerry (inačica 6.0.0 i niže).

Metoda napada

- Gruba sila – programska potpora za stvaranje sigurnosne kopije podataka na uređaju koristi slabu lozinku za šifriranje uređaja koju je moguće u kratkom vremenu pogoditi korištenjem dostupnih alata za pogađanje šifri. Napad je moguće obaviti samo lokalno, nema mogućnosti za udaljeni pristup.

Ranjivost koja se iskorištava

- Greška u dizajnu – korištenjem slabe lozinke za šifriranje podataka omogućuje se izvođenje napada grubom silom (engl. Brute-Force).

Microsoft ClickOnce

Svrha napada

- Dobivanje informacija – napadač želi presresti osjetljive informacije (kao korisničke lozinke) koje će mu omogućiti daljnji napad na sustav.

Meta napada

- Računalni sustav – iskorištavanjem prikupljenih informacija napadač može povećati prava pristupa i izvršavati proizvoljne napade na računalu žrtvi.

Metoda napada

- Prisluškivanje – iskorištavanjem brojnih ranjivosti napadač može prisluškivati komunikaciju između proizvoljnih računala na mreži.

Ranjivost koja se iskorištava

- ListaGreška u dizajnu – postoje brojne greške u dizajnu protokola za komunikaciju i autentifikaciju računala u komunikaciji. Napadač može iskoristiti neku od njih kako bi presreo komunikaciju. Jedna od najlakših metoda napada je umetanje vlastitih .dll datoteka micanjem odgovarajućih atributa za provjeru integriteta – u slučaju kada ne postoji sažetak računalo će i dalje obraditi zahtjev. Više o ostalim napadima može se naći na adresi: http://packetstormsecurity.org/files/view/91970/clickonce-mitm.txt

From:
https://www.cis.hr/WikiIS/ - **wikiIS**

Permanent link:
https://www.cis.hr/WikiIS/doku.php?id=klasifikacija_napada

Last update: **2015/01/21 13:37**