OpenSSL pod povećalom

Nakon što je otkriven Hartbleed bug, krenula je žestoka revizija koda tog popularnog i masovno korištenog sigurnosnog alata. Pogađate, otkrivene su greške koje su godinama "spavale" u kodu.

Tako je OpenBSD developer Ted Unangst, proučavajući načine sprečavanja Harbleed ranjivosti, primijetio da su u kodu aktivne funkcije čija je namjena izbjegavanje exploita. Kad ih je isključio, kod se više nije dao kompilirati. To bi samo po sebi bilo bizarno iskustvo, ali zabava tu ne prestaje. Unangst je otkrio kako su programeri davnih dana, dok je funkcija *malloc()* bila spora, smislili način da zaobiđu problem. Umjesto da se popravi *malloc()*, oni su smislili prečicu za oslobađanje zauzete memorije: LIFO listu otvorenih konekcija (*Last In, First Out*). U međuvremenu su se pojavile poboljšane verzija *malloca*, ali zaobilazni kod se nitko nije sjetio izbaciti. Kako to obično biva, rješenje problema izvor je novih problema, pa su tako napadači dobili mogućnost da nova konekcija preuzme buffer prethodne, koji nije propisno očišćen, ali i rušenja OpenSSL servisa. Ispravak nije bio kompliciran, pa su već izdane zakrpe.

Ubuntu je riješio problem, što se vidi iz njihovog priopćenja [1]. Upada u oči da je problem uočen još prije četiri godine, ali nije riješen, pa je zatim ponovo prijavljen:

```
It was discovered that OpenSSL incorrectly handled memory in the
ssl3_read_bytes() function. A remote attacker could use this issue to
possibly cause OpenSSL to crash, resulting in a denial of service.
(CVE-2010-5298 [2])

It was discovered that OpenSSL incorrectly handled memory in the
do_ssl3_write() function. A remote attacker could use this issue to
possibly cause OpenSSL to crash, resulting in a denial of service.
(CVE-2014-0198 [3])
```

Debian je 17.4.2014. objavio da su i oni riješili problem, a i na njihovoj se stranici se vidi da je prijavljen još 2010. :(

https://www.debian.org/security/2014/dsa-2908 [4]

Ako je trebalo četiri godine da se ispravi greška u otvorenom kodu, možemo samo spekulirati o greškama koje spavaju u zatvorenom, vlasničkom kodu. Sve u svemu, živimo s greškama u softveru kojeg svakodnevno koristimo, samo je pitanje tko će ih prije otkriti, "loši dečki", koji se njima žele okoristiti, ili "dobri dečki", koji ih ne zloupotrebljavaju i nastoje će da se one što prije isprave.

sri, 2014-05-07 06:29 - Aco Dmitrović**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1394

Links
[1] http://www.ubuntu.com/usn/usn-2192-1
[2] http://people.canonical.com/~ubuntu-security/cve/2010/CVE-2010-5298.html
[3] http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html
[4] https://www.debian.org/security/2014/dsa-2908