TLP:GREEN
Korlátozottan terjeszthető!

Tájékoztatás
A Diffie-Hellman titkosítás kihasználása processzor túlterhelés céljából

(2021. november 18.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban: NBSZ NKI) **tájékoztatást** ad ki a Diffie-Hellman **CVE-2002-20001** számú sebezhetőséggel kapcsolatosan.

Diffie-Hellman kriptográfia

A BalaSys IT Kft. 2021.11.08-án tartott előadása során demonstrálta a Diffie-Hellman kulcsmegállapodási protokollt érintő kutatásuk eredményét. A Diffie-Hellman kulcscsere (továbbiakban DHE) egy népszerű kriptográfiai algoritmus, amely lehetővé teszi az internetes protokollok számára, hogy megállapodjanak egy közös kulcsban, és biztonságos kapcsolatról kommunikáljanak egymással, amely algoritmust 1967-ben publikálták.

A Diffie-Hellman kulcscsere a nyilvános kulcsú kriptográfia egyik legfontosabb fejlesztése volt, és a mai napig gyakran alkalmazzák a különböző biztonsági protokollokban. Alapvető fontosságú az olyan protokollok számára, mint:

- Hypertext Transport Protocol Secure (HTTPS),
- Secure Shell (SSH),
- Internet Protocol Security (IPsec),
- Simple Mail Transfer Protocol Secure (SMTPS)
- és más, a Transport Layer Security (TLS) protokoll.

Diffie-Hellman processzorral kapcsolatos sérülékenység

A Diffie-Hellman kulcsmegállapodási protokoll lehetővé teszi a távoli támadók számára (a kliens oldaláról), hogy tetszőleges számokat küldjenek, amelyek valójában nem nyilvános kulcsok, és költséges szerveroldali DHE moduláris-önellentételes számításokat, azaz D(HE)ater-támadást indítsanak. Az ügyfélnek nagyon kevés CPU-erőforrásra és hálózati sávszélességre van szüksége. A támadás zavaróbb lehet olyan esetekben, amikor az ügyfél megkövetelheti a kiszolgálótól, hogy válassza ki a legnagyobb támogatott kulcsméretet. Az alapvető támadási forgatókönyv az, hogy az ügyfélnek azt kell állítania, hogy csak DHE-vel tud kommunikálni, a kiszolgálót pedig úgy kell konfigurálni, hogy engedélyezze a DHE-t.

A D(HE)ater egy CPU-fűtésen alapuló támadási eszköz, amely a Diffie-Hellman kulcscsere (DHE) efemer változatát kényszeríti ki adott kriptográfiai protokollokban (pl. TLS, SSH). A kliensoldalon kriptográfiailag helyes efemer kulcs kiszámítása nélkül, de a szerveroldalon jelentős mennyiségű számítási kapacitást igényel a célzott szervertől. Erre alapozva egy szolgáltatásmegtagadási (DoS) támadás indítható, amelyet D(HE)ater támadásnak nevezünk.

A támadás kivitelezése viszonylag egyszerű. Olyan üzenetet kell küldeni a szerver felé, amely egy olyan kliens látszatát kelti, amely csak DHE kulcscserét támogat. Ennek hatására a szerver olyan, a kulcscseréhez szükséges számításokba kezd, amelyek kifejezetten CPU intenzívek. TLS esetén ehhez egyetlen üzenet (ClientHello) elküldése is elegendő, SSH esetén ugyanehhez legalább 3 üzenet küldésére és 2 üzenet fogadására van szükség, viszont míg TLS esetén a kulcsméret, amelynek növelésével a számításiigény is nő, a szerver által meghatározott, addig SSH esetén a kulcsméretet a kliens tudja befolyásolni, a szerver beállításainak megfelelő határok között, amely praktikusan azt jelenti, hogy míg TLS esetén a legelterjedtebb a 2048 bites kulcsméret, addig SSH esetén a 8192 kulcsméret jellemzően kikényszeríthető, ezzel növelve a támadás hatékonyságát.

A támadás, TLS esetén akár 6-7 KB/s sávszélesség felhasználásával képes egy 1 CPU-n 100% terhelést elérni. Maga a támadás különböző hatékonysággal, de működik SSH és IPSec esetén is, egyelőre a DHEATER tool csak SSH-t támogat, ahol ~80 KB/s szükséges a 100% CPU terhelés eléréséhez.

Javaslat

A Diffie-Hellman nyilvános kulcscserélő algoritmus helyes üzembe helyezésére a TLS-hez a következőket javasoljuk:

Ha szervert futtat:

Ha web- vagy levelezőkiszolgálóval rendelkezik, tiltsa le a titkosítási csomagok exportálásának támogatását, és használjon 2048 bites vagy erősebb Diffie-Hellman titkosítást.

Ha SSH-t használ, frissítse mind a kiszolgáló, mind az ügyféltelepítéseket az OpenSSH legújabb verziójára, amely az Elliptic-Curve Diffie-Hellman Key Exchange-t részesíti előnyben. Elliptic-Curve Diffie-Hellman (ECDH) kulcscsere elkerüli az összes ismert megvalósítható kriptoanalitikus támadást.

Ha böngészőt használ:

Győződjön meg arról, hogy telepítve van a böngésző legújabb verziója, és gyakran ellenőrizze a frissítéseket.

Tiltsa le a Titkosítási csomagok exportálását. A modern böngészők már nem támogatják az exportcsomagokat, a FREAK és a Logjam támadások lehetővé teszik egy köztes támadó számára, hogy becsapja a böngészőket az export minőségű kriptográfia használatával, így a TLS-kapcsolat visszafejthető.

A Google Chrome (beleértve az Android böngészőt is), a Mozilla Firefox, a Microsoft Internet Explorer és az Apple Safari böngészők legfrissebb verzióinak telepítését javasoljuk, melyek már tartalmazzák a Logjam támadás javítását.

Ha Ön admin vagy fejlesztő:

Győződjön meg arról, hogy az Ön által használt TLS-tárak naprakészek, a karbantartott kiszolgálók 2048 bites vagy nagyobb titkosítást használnak, és hogy a fenntartott ügyfelek elutasítják az 1024 bitesnél kisebb Diffie-Hellman titkosítást.

Hivatkozások

- https://weakdh.org/
- https://weakdh.org/sysadmin.html
- https://snailman.web.elte.hu/pub/diffie-hellman/diffie-hellman/dh-f2.htm
- https://www.researchgate.net/figure/Message-Sequence-Chart-of-the-Logjam-attack-Source-1_fig1_301874824
- https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042015
- https://pythonawesome.com/a-security-tool-can-perform-dos-attack-by-enforcing-the-dhe-key-exchange/
- https://cacm.acm.org/magazines/2019/1/233523-imperfect-forward-secrecy/fulltext
- https://nvd.nist.gov/vuln/detail/CVE-2002-20001
- https://www.ssllabs.com/ssltest/
- https://github.com/Balasys/dheater
- https://hup.hu/cikkek/20211011/diffie_hellman_kulcscseret_tamogato_szerverek_tulterhelese