TLP: WHITE
Szabadon terjeszthető!

Tájékoztatás

PGP kulcskiszolgáló elleni támadásról

(2019. július 24.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki arra vonatkozóan, hogy 2019. június végén ismeretlen támadók kompromittált PGP kulcsok felhasználásával rávilágítottak az OpenPGP protokoll hiányosságaira. A médiában több helyen a PGP titkosítás végét vetítették előre. A támadás azonban nem a PGP titkosítás feltörését jelentette, hanem az OpenPGP protokoll tervezési „hibájának" kihasználása által a GnuPG kliens túlterheléssel előidézett leállását.

Történeti áttekintés

A PGP-t (Pretty Good Privacy) az 1990-es évek elején fejlesztették ki. Célja egy olyan titkosítás létrehozása volt, amely erős védelmet nyújt és a nyilvánosság számára is elérhető. A nyilvános tanúsítványok (melyek tartalmazzák a publikus kulcsot) terjesztésére speciális rendszereket, úgynevezett kulcskiszolgálókat létesítettek. Ezen kulcskiszolgálók egyike, az úgynevezett SKS Kulcskiszolgáló (Synchronizing Key Server). Annak érdekében, hogy a tanúsítványokat ne lehessen lecserélni vagy eltávolítani, az SKS kulcskiszolgálókat úgy alakították ki, hogy a bennük lévő tanúsítványokat, illetve a rájuk vonatkozó információkat soha ne lehessen törölni. Ehhez arra volt szükség, hogy a kulcskiszolgálók hálózatba kapcsolódjanak, ahol egymással folyamatosan kommunikálnak, a rajtuk tárolt adatokat rendszeresen szinkronizálják. Ez biztosítja, hogy minden kulcskiszolgálón megtalálható legyen az összes tanúsítvány. A tanúsítványok bárki által, akár többször is aláírhatóak, azonban a kulcskiszolgáló nem ellenőrzi ezen aláírások hitelességét, azokat a felhasználóra bízza.

Az OpenPGP protokoll hiányosságának kihasználása

Ismeretlen támadók a PGP közösség két prominens tagjának (Robert J. Hansen és Daniel Kahn Gillmor) SKS kulcskiszolgálón lévő tanúsítványait kompromittálták oly módon, hogy azokat csaknem százötvenezer aláírással látták el. Az SKS kulcskiszolgáló ugyanis a korábban leírt sajátosságai miatt, lehetővé teszi a tanúsítványok ilyen nagy számban történő aláírását, azok hitelességét nem ellenőrzi és ezek a tanúsítványok nem is távolíthatóak el a kiszolgálóról. A GnuPG kliens az ily módon kompromittált tanúsítványok

importálása során túlterhelődik és ennek következtében elérhetetlenné válik. Az OpenPGP protokoll hiányosságának hátterében így egy olyan tervezési „hiba” áll, amely biztonsági frissítéssel nem orvosolható.

Javaslat

A veszélynek legjobban kitett felhasználók számára ajánlott az SKS kulcskiszolgálók használatának azonnali felfüggesztése. Emellett több megoldás is létezik arra, hogy a GnuPG szoftver túlterhelését és ennek következtében annak leállását elkerüljük.

Kevés PGP kulcs használata esetén, azok manuálisan is feltölthetőek.

Használható a néhány héttel ezelőtt bejelentett **OpenPGP kulcskiszolgáló**[1] is, amely ellenőrzi az e-mail címeket és egyszerű kezelhetőséget biztosít a kulcsok tulajdonosainak. Egy új kulcs feltöltése után a szerver e-mailt küld a kulcsban megadott összes e-mail címre. Ez az e-mail tartalmaz egy hivatkozást, amin keresztül a kulcs véglegesíthető. Ezután bárki, aki a kulcskiszolgálón rákeres egy adott e-mail címre, csak azokat a kulcsokat fogja látni, amit a tulajdonos valóban kiadott. Ráadásul ezek a kulcsok bármikor visszavonhatóak.

A kulcsszervereket ért szolgáltatásmegtagadásos támadások enyhítése érdekében kiadták a **GnuPG** szoftver legújabb **2.2.17**-es verzióját is. Az új verzióban számos változást eszközöltek, melyek közül az egyik legfontosabb, hogy figyelmen kívül hagyja a kulcskiszolgálótól kapott összes aláírást, így megakadályozza, hogy hamis aláírások tömegével működésképtelenné tegyék a programot.

További hivatkozások:

- https://nki.gov.hu/it-biztonsag/hirek/javithatatlan-hibat-fedeztek-fel-egy-nepszeru-pgp-kulcsszerver-halozatban/
- https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f
- https://dkg.fifthhorseman.net/blog/openpgp-certificate-flooding.html
- https://tools.ietf.org/html/draft-dkg-openpgp-abuse-resistant-keystore-03
- https://www.heise.de/security/meldung/Angriff-auf-PGP-Keyserver-demonstriert-hoffnugslose-Situation-4458354.html
- https://www.heise.de/security/meldung/Neuer-OpenPGP-Keyserver-liefert-endlich-verifizierte-Schluessel-4450814.html
- https://lists.gnupg.org/pipermail/gnupg-announce/2019q3/000439.html

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu

[1] https://sequoia-pgp.org/blog/2019/06/14/20190614-hagrid/