TLP:WHITE
Szabadon terjeszthető!

Rendkívüli tájékoztatás

a STARTTLS implementációit érintő biztonsági frissítésekkel kapcsolatban

(2021. május 28.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **rendkívüli tájékoztatót** ad ki a **STARTTLS implementációit érintő sérülékenységek frissítéseivel** kapcsolatban.

A sebezhetőségek lehetővé tehetik, hogy a támadók Man-in-the-Middle[1] (MITM) támadást indítsanak, amely a felhasználónév és jelszó ellopását eredményezheti. A hibák biztosíthatják a támadók számára, hogy az SMTP-munkamenetbe kliensparancsokat juttassanak be, amelynek köszönhetően módosíthatják a kommunikációt a két fél között.

Védelmi stratégiák:

A sérülékenységekben érintett gyártók csomagfrissítéseket tettek elérhetővé. A javításhoz elegendő lehet az infrastruktúrában lévő szerverszoftver frissítése, vagy megkerülő megoldásként a **STARTTLS** teljes kikapcsolása, és csak a 993/465/995-ös portokon történő TLS-kapcsolatok elfogadása.

A sérülékenységek az alábbi CVE azonosítókhoz köthetőek:

- Postfix (<2.7.3): CVE-2011-0411
- Ipswitch IMail (<11.03): CVE-2011-1430
- netqmail-1.06-tls: CVE-2011-1431
- SCO SCOoffice Server: CVE-2011-1432
- Kerio Connect (7.1.4) and MailServer (6.x): CVE-2011-1506
- Pure-FTPd (<1.0.30): CVE-2011-1575
- Cyrus IMAP Server (<2.4.7): CVE-2011-1926
- WatchGuard XCS 9.0 and 9.1: CVE-2011-2165
- spamdyke (<4.2.1): CVE-2012-0070
- nnrpd in INN (<2.5.3): CVE-2012-3523
- MailMarshal (<7.2): CVE-2014-2727
- nginx (1.5.x, 1.6.x-1.6.1, 1.7.x-1.7.4): CVE-2014-3556
- Synacor Zimbra Collaboration (<8.0.9): CVE-2014-8563
- s/qmail: CVE-2020-15955
- Coremail: No response from vendor
- Citadel: CVE-2020-29547
- Gordano GMS (IMAP/POP3): No CVE assigned
- SmarterMail (POP3): CVE-2020-29548
- Burp Collaboration Server: https://hackerone.com/reports/953219
- Mercury Mail Transport System: CVE-2021-33487

A STARTTLS-t alkalmazó szervezetek számára az NBSZ NKI javasolja a frissítések mielőbbi telepítését.

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

[1] https://en.wikipedia.org/wiki/Man-in-the-middle_attack