Upozorňujeme na hrozbu Terrapin útoku mířícího na SSH protokol

portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/upozornujeme-na-hrozbu-terrapin-utoku-miriciho-na-ssh-protokol

Na konci prosince 2023 došlo ke zveřejnění nového druhu útoku mířícího na SSH protokol – útok Terrapin, který využívá zranitelnosti CVE-2023-48795 (CVSS 5.9). Jedná se o prefix truncation attack, kdy útočník manipuluje daty při ustanovování komunikace tzv. handshake. Tím zapříčiní použití méně bezpečných algoritmů a deaktivaci některých bezpečnostních protiopatření.

Důležitým předpokladem je, aby byl útočník v pozici MitM (Man in the Middle). Spojení musí být zároveň zabezpečeno šifrou ChaCha20-Poly1305 nebo jakoukoliv CBC šifrou v kombinaci s Encrypt-then-Mac, které jsou velmi rozšířené.

V prostředí internetu je složité dostat se do pozice MitM. Proto útočníci často kompromitují síťovou infrastrukturu a vyčkávají na okamžik, kdy se objeví podobné zranitelnosti, aby mohli do infrastruktury proniknout hlouběji.

Bezpečnostní organizace Shadowserver Foundation nalezla rozsáhlým skenováním internetu skoro 11 milionů zranitelných SSH serverů. Informaci sdílela např. na sociální síti X (https://x.com/Shadowserver/status/1742482640815419653?s=20). Neznamená to, že jsou všechny tyto servery v nebezpečí, ale poukazuje to na rozsáhlost zranitelnosti.

Skener zranitelnosti na Terrapin útok od Ruhr-Universität Bochum: https://github.com/RUB-NDS/Terrapin-Scanner.

Mitigace

Většina vývojářů SSH klientů již vydala bezpečnou verzi, na kterou doporučujeme aktualizovat server i klienta. U některých se ale zatím jedná o beta-verzi např. WinSCP. Podrobný přehled zde: https://terrapin-attack.com/patches.html.

Pokud ještě není vydána aktualizace, doporučujeme v konfiguraci SSH pro klienta i server zakázat používání šifry Chacha20-Poly1305, jakékoliv Encrypt-then-MAC (EtM) a ověřit, že nejsou využívány žádné aes(128|192|256)-cbc. Příklad zakázání v /etc/ssh/ssh_config:

```
Ciphers -chacha20-poly1305@openssh.com
```

K nastavování konfigurace SSH doporučujeme přistupovat s opatrností, protože nesprávná konfigurace může způsobit ztrátu spojení se serverem.

Zdroje

- SSH Prefix Truncation Vulnerability Used in Terrapin Attacks (CVE-2023-48795) – Qualys ThreatPROTECT
- SSH shaken, not stirred by Terrapin downgrade vulnerability • The Register
- SSH protects the world's most sensitive networks. It just got a lot weaker | Ars Technica
- Nearly 11 million SSH servers vulnerable to new Terrapin attacks (bleepingcomputer.com)
- SSH Protocol Flaw CVE-2023-48795 Terrapin Attack: All You Need To Know (jfrog.com)
- CVE-2023-48795- Red Hat Customer Portal

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

05. 01. 2024

Obsah

Reakce

Zatím žádné reakce na článek