BEZPEČNOSTNÉ VAROVANIE

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

CallStranger Universal Plug and Play (UPnP) amplifikačný DDoS útok

Popis

Bezpečnostný výskumník informoval o zraniteľnosti zariadení podporujúcich funkciu Universal Plug and Play (UPnP), ktorá bola pomenovaná CallStranger.
Bezpečnostná zraniteľnosť vo funkcii UPnP SUBSCRIBE je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente vykonať amplifikačný DDoS útok s amplifikačným faktorom až 92 a taktiež získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.04.2020

CVE

CVE-2020-12695

Zasiahnuté systémy

IoT a periférne zariadenia používajúce funkciu UPnP SUBSCRIBE

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame aplikovať firewallové pravidlá a blokovať spojenia UPnP v súlade s dokumentáciou RFC1918. Tiež odporúčame sledovať stránky výrobcov zasiahnutých zariadení a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://callstranger.com
https://www.zdnet.com/article/callstranger-vulnerability-lets-attacks-bypass-security-systems-and-scan-lans/
https://www.tenable.com/blog/cve-2020-12695-callstranger-vulnerability-in-universal-plug-and-play-upnp-puts-billions-of

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01439/2020/SK-CERT-139