TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Ivanti termékeket érintő 0. napi kritikus sérülékenységekről

(2024. január 11.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki az **Ivanti Connect Secure és az Ivanti Policy Secure** szoftvereket érintő **0. napi, kritikus kockázati** besorolású sérülékenységek kapcsán, azok súlyossága és aktív kihasználása miatt.

A sérülékenységek az összes támogatott verziót - **9.x és 22.x** – érintik. A biztonsági rés lehetővé teszi a támadó számára a távoli kódfuttatást az Ivanti Connect Secure VPN eszközökön.

CVE-2023-46805: Az Ivanti Connect Secure (9.x, 22.x) és az Ivanti Policy Secure webes komponensének hitelesítés megkerülési sebezhetősége lehetővé teszi egy távoli támadó számára, hogy az ellenőrzések megkerülésével hozzáférjen korlátozott és bizalmas erőforrásokhoz.

CVE-2024-21887: Az Ivanti Connect Secure (9.x, 22.x) és az Ivanti Policy Secure webes komponenseiben lévő parancsinjekciós (command injection) sebezhetőség lehetővé teszi, hogy egy hitelesített rendszergazda speciális kéréseket küldjön és tetszőleges parancsokat hajtson végre a készüléken.

Javasolt intézkedések

Hivatalos javítás egyelőre még nem áll rendelkezésre, viszont a gyártó a rendszergazdák számára a sebezhetőség csökkentése érdekében javasolja a *mitigation.release.20240107.1.xml* fájl importálását. A letöltés hatással lehet egyes rendszerfunkciók működésére, erről a gyártó honlapján részletes tájékoztató olvasható.

A hivatalos javítás megjelenéséig Intézetünk azt javasolja, hogy az érintett ügyfelek hajtsák végre a mérséklő intézkedéseket, figyeljék a gyártó honlapját és amennyiben hivatalos javítás elérhetővé válik, azonnal telepítsék.

TLP:CLEAR
Szabadon terjeszthető!

Hivatkozások:

- https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2023-46805/
- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

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

NEMZETI
KIBERVÉDELMI INTÉZET