TLP:CLEAR
Szabadon terjeszthető!

Tájékoztatás

Ivanti termékeket érintő sérülékenységekről

(2024. november 15.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki **Ivanti Endpoint Manager (EPM), Ivanti Avalanche, Ivanti Connect Secure, Ivanti Policy Secure,** és **Ivanti Security Access Client** szoftvertermékeket érintő, **kritikus kockázati besorolású** sérülékenységek kapcsán, azok súlyossága és kihasználhatósága miatt.

Az **Ivanti Endpoint Managert (EPM)** több magas és egy **kritikus kockázati besorolású** sérülékenység érinti (CVE-2024-50330), amely SQL injection támadás során kihasználható távoli kódfuttatásra.

Termék:	Érintett verziók:	Javított verziók	Patch elérése:
Ivanti Endpoint Manager (EPM)	**2024 September security update és korábbi verziók,** **2022 SU6 és korábbi verziók**	**2024 November Security Update, 2022 SU6 November Security Update**	**EPM 2024 November Patch** **EPM 2022 SU6 November Patch**

A gyártói biztonsági közlemény itt érhető el: https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022?language=en_US

Az **Ivanti Avalanche** kapcsán **öt magas kockázati besorolású** sebezhetőség került javításra, amelyek Denial-of-Service támadásra használhatók fel.

Termék:	Érintett verziók:	Javított verzió:	Patch elérése:
Ivanti Avalanche	**6.4.5 és korábbi verziók**	**6.4.6**	**Download Portal**

A gyártói biztonsági közlemény itt érhető el: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-Multiple-CVEs-Q4-2024-Release?language=en_US

Az **Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Ivanti Secure Access Client (ISAC)** szoftvertermékek esetében több kritikus kockázati besorolású sebezhetőség autentikált támadó számára távoli kódfutattást tehet lehetővé. Egyes magas és közepes kockázati besorolású biztonsági hibák sikeres kihasználás esetén és Denial-of-Service kondíciót eredményezhetnek.

TLP:CLEAR
Szabadon terjeszthető!

Termék:	Érintett verziók:	Javított verzió:	Patch elérése:
Ivanti Connect Secure (ICS)	**22.7R2.2 and prior**	**22.7R2.3**	**Ivanti Portal**
Ivanti Policy Secure (IPS)	**22.7R1.1 and prior**	**22.7R1.2**	**Ivanti Portal**
Ivanti Secure Access Client (ISAC)	**22.7R3 and prior**	**22.7R4**	**Ivanti Portal**

A gyártói biztonsági közlemény itt érhető el: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-Multiple-CVEs-Q4-2024-Release?language=en_US

Az NBSZ NKI a gyártó által kiadott biztonsági frissítések haladéktalan telepítését javasolja.

Hivatkozások:

- https://www.cisa.gov/news-events/alerts/2024/11/12/ivanti-releases-security-updates-multiple-products

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