TLP:CLEAR
Szabadon terjeszthető!

Riasztás

Ivanti terméket érintő kritikus sérülékenységről

Tisztelt Ügyfelünk!

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) riasztást ad ki az **Ivanti Endpoint Manager (EPM)** szoftvert érintő **kritikus** kockázati besorolású **sérülékenység** kapcsán.

A **CVE-2025-10573** azonosítón nyomon követett, **stored cross-site scripting (XSS)** sérülékenység, (CVSS pontszáma 9,6), az **Ivanti EPM 2024 SU4** és annál **korábbi verzióit** érinti.

A sebezhetőség kihasználásával egy nem hitelesített támadó, manipulált végpontokat képes létrehozni az EPM szerveren, amelyek a rendszer számára legitim menedzselt eszközként jelennek meg. Ez rosszindulatú JavaScript kódfuttatást tehet lehetővé az admin irányítópult felületén. Amikor az Ivanti EPM adminisztrátor a megszokott használat során megnyitja a kompromittált irányítópultot, a pusztán passzív felhasználói interakció is elegendő a kliensoldali JavaScript-kód végrehajtásához, amely végső soron lehetővé teszi a támadó számára az adminisztrátori munkamenet átvételét.

Az Ivanti 2025. december 9-én az **Ivanti EPM 2024 SU4 SR1 verzió** kiadásával **javította** a sérülékenységet. Mivel a sebezhetőség **hitelesítés nélkül is kihasználható**, **javasolt az érintett rendszerek mielőbbi frissítése.**

Hivatkozások:

ivanti.com

rapid7.com

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833