



AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Dobësi të Shumta në Ivanti Endpoint Manager 2024

Data: 11/02/2026

Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	1
Informacione Teknike	1
Rekomandime	2
Referenca	2

Përmbledhje Ekzekutive

Ivanti ka publikuar përditësimin e sigurisë **version 2024 SU5**, i cili adreson disa dobësi në Ivanti Endpoint Manager që mund të lejojnë sulmues nga distanca të komprometojnë sistemet dhe të nxjerrin të dhëna sensitive.

Dobësia më serioze (**CVE-2026-1603**) është vlerësuar **8.6 – HIGH**, dhe u mundëson sulmuesve të paautentikuar të:

- Anashkalojnë autentikimin
- Ekspozojnë kredenciale të ruajtura

Një dobësi e dytë (**CVE-2026-1602**) u mundëson sulmuesve të autentikuar të kryejnë sulme **SQL Injection**, duke lexuar informacion arbitrar nga databaza.

Informacione Teknike

Pikat Kryesore

- 2 dobësi të reja të zbuluara (1 HIGH, 1 MEDIUM)
- 11 dobësi të tjera me rrezikshmëri mesatare nga tetori 2025 janë zgjidhur

Detaje të Dobësive

1. CVE-2026-1603: Anashkalim Autentikimi që Çon në Ekspozim Kredencialesh

- **Rrezikshmëria:** HIGH (CVSS 8.6)

2. CVE-2026-1602: Dobësi SQL Injection

- **Rrezikshmëria:** MEDIUM (CVSS 6.5)

Sistemet e Prekura

- **Produkti i prekur:** Ivanti Endpoint Manager (EPM)
- **Versionet e prekura:** 2024 SU4 SR1 dhe të gjitha versionet para tij
- **Versioni i rregulluar:** 2024 SU5

Rekomandime

AKSK rekomandon të:

- Aplikoni menjëherë përditësimet e sigurisë.
- Jepni prioritet instalimeve EPM që janë të ekspozuara në internet ose publikisht të aksesueshme.

Referenca

https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US