AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësimi i Sigurisë së Ivanti EPMM: Shfrytëzimi aktiv i CVE-2026-6973 dhe dobësi të shumëfishta me ashpërsi të lartë

Data: 08/05/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Ivanti ka publikuar përditësime sigurie për Endpoint Manager Mobile (EPMM) duke adresuar pesë dobësi me rëndësi të lartë, duke përfshirë CVE-2026-6973, i cili është konfirmuar se është shfrytëzuar në mënyrë aktive në sulme të kufizuara në terren. Ky defekt i lejon një administratori të autentifikuar nga distanca të arrijë ekzekutimin e kodit nga distanca në kushte specifike.

Informacione Teknike

Ivanti konfirmoi shfrytëzimin aktiv, në raste të kufizuara, të dobësisë CVE-2026-6973, e cila kërkon autentifikim administrativ. Gjithashtu, Ivanti rekomandon që infrastrukturat e prekura më parë nga dobësitë e janarit 2026 (CVE-2026-1281 dhe CVE-2026-1340) të sigurohen që procesi i rotacionit të kredencialeve të jetë përfunduar, për të reduktuar rrezikun e shfrytëzimit të mëtejshëm.

Detajet e Dobësive

• **CVE-2026-5786**
Ashpërsia / CVSS: E lartë — 8.8
Dobësi e kontrollit të papërshtatshëm të qasjes që i lejon një sulmuesi të autentifikuar në distancë, me privilegje të ulëta, të fitojë qasje administrative në Ivanti EPMM.

• **CVE-2026-5787**
Ashpërsia / CVSS: E lartë — 8.9
Dobësi e validimit të papërshtatshëm të certifikatës që i lejon një sulmuesi të paautorizuar në distancë të imitojë hostet e regjistruara Sentry dhe të marrë certifikata të vlefshme klientësh të nënshkruara nga CA.

• **CVE-2026-5788**
Ashpërsia / CVSS: E lartë — 7.0
Dobësi e kontrollit të papërshtatshëm të qasjes që i lejon një sulmuesi të paautorizuar në distancë të përdorë metoda arbitrare.

• **CVE-2026-6973**
Ashpërsia / CVSS: E lartë — 7.2
Dobësi e validimit të papërshtatshëm të hyrjes që i lejon një sulmuesi të autentifikuar në distancë, me privilegje administrative, të arrijë ekzekutimin e kodit në distancë (RCE). Ivanti ka raportuar raste të kufizuara të shfrytëzimit aktiv në terren.

• **CVE-2026-7821**
Ashpërsia / CVSS: E lartë — 7.4
Dobësi në validimin e certifikatës që i lejon një sulmuesi të paautorizuar në distancë të regjistrojë një pajisje nga një grup i kufizuar pajisjesh të paregjistruara, duke çuar potencialisht në zbulimin e informacionit mbi pajisjen EPMM dhe kompromet imin e integritetit të identitetit të pajisjes.

Produktet e Prekura

• Ivanti Endpoint Manager Mobile (EPMM)

Versionet e Prekura

• 12.8.0.0 dhe versionet e mëparshme

Versionet e Përditësuara

• 12.6.1.1
• 12.7.0.1
• 12.8.0.1

Këto versione përfshijnë gjithashtu rregullime për dobësitë:

• CVE-2026-1281
• CVE-2026-1340

Sentry

Versionet e reja të disponueshme:

• 10.4.2
• 10.5.1
• 10.6.1

Përditësimi i Sentry është opsional, përveç rasteve kur po vendoset një instancë e re Sentry.

Rekomandime

AKSK rekomandon :

• Zbatoni menjëherë përditësimet e sigurisë të ofruara nga Ivanti EPMM
• Verifikoni dhe zbatoni kontrolle të forta të vërtetimit administrativ
• Ndërroni kredencialet administrative, veçanërisht nëse dyshohet për kompromentim të mëparshëm
• Rishikoni regjistrat për aktivitet administrativ të paautorizuar ose përdorim të dyshimtë të API-t
• Monitoroni lëshimin e certifikatave dhe aktivitetin e regjistrimit të pajisjes për anomali
• Kufizoni aksesin administrativ në rrjete/diapazone IP të besuara aty ku është e mundur

Referenca

- https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US