AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi Kritike në IBM Common Cryptographic Architecture (CCA)

Data: 10/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 1
Referenca 1

Përmbledhje Ekzekutive

Është identifikuar një dobësi kritike në IBM Common Cryptographic Architecture (CCA), e cila përdoret për të ndërvepruar me IBM Hardware Security Modules (HSMs). Kjo dobësi mund t'i lejojë një sulmuesi të paautentikuar nga distanca të ekzekutojë komanda arbitrare me privilegje të ngritura, duke çuar në ndikim të rëndë në sistemet e prekura.

Informacione Teknike

Detaje të Dobësisë

- **CVE:** CVE-2025-13375
- **CVSS v3.1 Base Score:** 9.8 (Kritike)
- **CWE:** CWE-250 – Ekzekutim me privilegje të panevojshme
- **Përshkrim teknik:** IBM Common Cryptographic Architecture (CCA) përmban një defekt që mund të lejojë një sulmues të paautentikuar nga distanca të ekzekutojë komanda arbitrare me privilegje të ngritura në sistemin e prekur. Shfrytëzimi me sukses mund të rezultojë në kompromet im të plotë të konfidencialitetit, integritetit dhe disponueshmërisë.

Produktet e Prekura

- **CCA 7 MTM për 4769** – versionet para 7.5.53
- **CCA 8 MTM për 4770** – versionet para 8.4.84
- **IBM 4769 Developers Toolkit** – versionet para 7.5.53
- **Platformat:** IBM AIX, IBM i, IBM PowerLinux, Linux (Intel x86)

Versionet e Rregulluara

- **CCA 7 MTM për 4769:** Përditësim në versionin 7.5.53
- **CCA 8 MTM për 4770:** Përditësim në versionin 8.4.84
- **IBM 4769 Developers Toolkit:** Përditësim në versionin 7.5.53
- **IBM i:** Aplikoni PTF-të përkatëse të IBM i për versionet e prekura, sipas udhëzimeve të IBM

Rekomandime

AKSK rekomandon **përditësimin e menjëhershëm** të versioneve të prekura në versionet e rregulluara ose më të fundit të publikuara nga **IBM**.

Referenca

https://www.ibm.com/support/pages/node/7259625