AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi Kritike në Cisco Integrated Management Controller (IMC)

Data: 02/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 3
Referenca 3

Përmbledhje Ekzekutive

Një dobësi kritike (**CVE-2026-20093, CVSS 9.8**) është identifikuar në Cisco IMC që lejon sulmues të paautentikuar në distancë të anashkalojnë autentikimin dhe të fitojnë akses të plotë administrativ.

Informacione Teknike

Detaje të Dobësisë:

- **CVE ID:** CVE-2026-20093
- **CWE:** CWE-20 (Validim i pasaktë i input-it)
- **CVSS v3.1:** 9.8 (Kritike)
- **Vektori:** AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:H

Shkaku Kryesor

- Validim dhe trajtim i pasaktë i kërkesave për ndryshim fjalëkalimi
- Mungesë e zbatimit të autentikimit gjatë operacioneve sensitive

Vektori i Sulmit

- Sulmues në distancë, pa autentikim, dërgon kërkesë HTTP të manipuluar
- Shfrytëzon endpoint-in e ndryshimit të fjalëkalimit
- Fiton akses të paautorizuar duke rivendosur kredencialet

Ndikimi

- Anashkalim i plotë i autentikimit
- Modifikim i paautorizuar i fjalëkalimeve (përfshirë llogaritë admin)

Produktet e Prekura

Infrastrukturë bazë:

- Cisco 5000 Series ENCS
- Cisco Catalyst 8300 Series Edge uCPE
- Cisco UCS C-Series M5 & M6 (modalitet standalone)
- Cisco UCS E-Series M3 & M6

Pajisje Cisco të ndikuara (nëse IMC UI është i ekspozuar):

Përfshin, por nuk kufizohet në:

- Serverët Application Policy Infrastructure Controller (APIC)
- Pajisjet Business Edition 6000 dhe 7000
- Pajisjet Catalyst Center
- Pajisjet Cisco Telemetry Broker
- Cloud Services Platform (CSP) 5000 Series
- Common Services Platform Collector (CSPC)
- Pajisjet Connected Mobile Experiences (CMX)
- Serverët Connected Safety and Security UCS Platform Series
- Pajisjet Cyber Vision Center
- Pajisjet Expressway Series
- HyperFlex Edge Nodes

Pajisje të tjera të ndikuara:

- HyperFlex Nodes në HyperFlex Datacenter pa Fabric Interconnect
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 Appliances
- Meeting Server 1000 Appliances
- Nexus Dashboard Appliances
- Prime Infrastructure Appliances
- Prime Network Registrar Jumpstart Appliances
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center Appliances
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server Appliances
- Secure Workload Servers

Nuk Preken

- UCS B-Series Blade Servers
- UCS C-Series M7 dhe M8 (standalone)
- UCS C-Series me Fabric Interconnect në UCS Manager ose Intersight
- UCS S-Series Storage Servers
- UCS X-Series Modular System
- Unified Edge

Versionet e Korrigjuara

- **UCS C-Series M5:** 4.3(2.260007)
- **UCS C-Series M6:** 4.3(6.260017), 6.0(1.250174)
- **UCS E-Series M3:** 3.2.17
- **UCS E-Series M6:** 4.15.3
- **Cisco NFVIS Catalyst 8300 uCPE:** 4.18.3
- **Cisco NFVIS 5000 Series ENCS:** 4.15.5

Shënim: Disa platforma kërkojnë përditësim NFVIS ose firmware bundle (HUU / ISO), jo vetëm patch direkt të IMC.

Rekomandime

Rekomandohet të:

- Aplikoni menjëherë patch-et në të gjitha sistemet e prekura
- Përditësoni në versionet e rekomanduara nga Cisco
- Verifikoni kryerjen e përditësimit pas implementimit

Referenca

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn