مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Cisco

Tracking #:432318466

Date:27-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Cisco has released security updates to address multiple vulnerabilities affecting several Cisco networking and infrastructure products. These vulnerabilities could allow an authenticated or unauthenticated attacker to perform authentication bypass, privilege escalation, remote code execution, cross-site scripting, or cause denial of service conditions.

Vulnerabilities Details
Critical Severity

- Cisco Catalyst SD-WAN Software — Multiple Vulnerabilities
  - CVE-2026-20122
  - CVE-2026-20126
  - CVE-2026-20128

High Severity

- Cisco SD-WAN Software — Privilege Escalation
  - CVE-2022-20775
  - CVE-2022-20818
- Cisco Nexus 3600 and 9500-R Series Switching Platforms — Layer 2 Loop DoS Vulnerability
  - CVE-2026-20051
- Cisco Nexus 9000 Series Fabric Switches (ACI Mode) — SNMP Denial of Service
  - CVE-2026-20048
- Cisco Nexus 9000 Series Fabric Switches (ACI Mode) — Denial of Service
  - CVE-2026-20033
- Cisco NX-OS Software — Link Layer Discovery Protocol Denial of Service
  - CVE-2026-20010

Medium Severity

- Cisco UCS Manager Software — Command Injection
  - CVE-2026-20036
- Cisco UCS Manager Software — Privilege Escalation
  - CVE-2026-20037
- Cisco FXOS and UCS Manager Software — Stored Cross-Site Scripting
  - CVE-2026-20091
- Cisco FXOS and UCS Manager Software — Command Injection
  - CVE-2026-20099
- Cisco Application Policy Infrastructure Controller — Denial of Service
  - CVE-2026-20107

Impact
Successful exploitation of these vulnerabilities may allow attackers to:

- Bypass authentication controls
- Execute arbitrary commands
- Escalate privileges
- Disrupt network services through denial of service
- Inject malicious scripts

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/publicationListing.x