مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Cisco ISE & Webex

Tracking #:432318796

Date:16-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple critical vulnerabilities have been disclosed by Cisco affecting Cisco Identity Services Engine (ISE), ISE Passive Identity Connector (ISE-PIC), and Cisco Webex Services.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been disclosed by Cisco affecting Cisco Identity Services Engine (ISE), ISE Passive Identity Connector (ISE-PIC), and Cisco Webex Services.

Vulnerability Details:

1. Cisco ISE RCE & Path Traversal

Affected Systems

- Cisco ISE (all deployments)
- Cisco ISE-PIC
- **CVE-2026-20147 (Critical – CVSS 9.9)**
  - Remote Code Execution
  - Requires admin credentials
  - Root cause: insufficient input validation
  - Attack vector: crafted HTTP request
  - Impact:
    - Arbitrary command execution
    - Privilege escalation to root
    - Node crash → Denial of Service (DoS)
    - Network authentication disruption
- **CVE-2026-20148 (Medium – CVSS 4.9)**
  - Path Traversal
  - Requires admin credentials
  - Root cause: improper input validation
  - Attack vector: crafted HTTP request
  - Impact:
    - Read sensitive system files
    - Potential credential exposure

Fixed Versions

- 3.1 → Patch 11
- 3.2 → Patch 10
- 3.3 → Patch 11
- 3.4 → Patch 6
- 3.5 → Patch 3

2. Cisco ISE Additional RCE Vulnerabilities

Affected Systems

- Cisco ISE only (ISE-PIC not affected)

Vulnerabilities

- **CVE-2026-20180 / CVE-2026-20186 (Critical – CVSS 9.9)**
  - Remote Code Execution
  - Requires Read-Only Admin privileges (lower barrier)
  - Root cause: insufficient input validation

- Attack vector: crafted HTTP request
- Impact:
  - OS command execution
  - Privilege escalation to root
  - Full system compromise
  - DoS in single-node deployments

Fixed Versions

- 3.2 → Patch 8
- 3.3 → Patch 8
- 3.4 → Patch 4
- 3.5 → Not vulnerable

3. Cisco Webex SSO Certificate Validation Vulnerability

Affected Systems

- Cisco Webex Services (SSO-enabled environments)

Vulnerability

- **CVE-2026-20184 (Critical – CVSS 9.8)**
  - Authentication Bypass / Impersonation
  - Requires no authentication
  - Root cause: improper certificate validation
  - Attack vector: crafted SSO token
  - Impact:
    - Impersonate any user
    - Unauthorized access to Webex services
    - Potential data exposure & account takeover

Fix Status

- Patched by Cisco (cloud-side)
- Customer action required: Update SAML IdP certificate

RECOMMENDATIONS:

- **Patch Immediately**
  - Upgrade Cisco ISE/ISE-PIC to fixed versions listed above
  - Validate patch success across all nodes
- **Webex SSO Remediation**
  - Upload new IdP SAML certificate in Control Hub
  - Verify certificate trust chain and expiration

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/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ