

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Active Exploitation of Critical Cisco ISE Vulnerabilities
Tracking #:432317536
Date:24-07-2025

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has issued an urgent warning that three recently patched critical remote code execution (RCE) vulnerabilities in Cisco Identity Services Engine (ISE) are now being actively exploited in the wild. immediate patching is strongly advised.

TECHNICAL DETAILS:

Multiple critical remote code execution (RCE) vulnerabilities in Cisco Identity Services Engine (ISE) are now being actively exploited in the wild. These vulnerabilities are rated as maximum severity (CVSS 10.0), are remotely exploitable without authentication, and could allow attackers to execute arbitrary code as root on affected systems.

Vulnerabilities Details:

- **CVE-2025-20281**
Unauthenticated Remote Code Execution
Allows attackers to send crafted API requests to execute arbitrary commands as root on the underlying OS without authentication.
- **CVE-2025-20282**
Unauthenticated Arbitrary File Upload and Execution
Enables attackers to upload malicious files into privileged directories due to a lack of file validation, resulting in code execution as root.
- **CVE-2025-20337**
Unauthenticated Remote Code Execution
Caused by insufficient input validation in API requests, allowing execution of arbitrary code as root.

Recommended Actions:

- **Patch Immediately**
 - ISE 3.3: Upgrade to Patch 7.
 - ISE 3.4: Upgrade to Patch 2.
 - No workarounds exist—patching is the only effective remediation.

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/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6>