مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Update-Critical Vulnerabilities Cisco Products

Tracking #:432315605

Date:12-02-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco has released security patches to address two critical vulnerabilities, CVE-2024-20252 and CVE-2024-20254, affecting its Expressway series devices. These vulnerabilities could be exploited remotely, without authentication, to launch cross-site request forgery (CSRF) attacks. The updates also address CVE-2024-20255, a high-severity CSRF vulnerability that enables remote, unauthenticated attackers to modify configurations and trigger denial-of-service (DoS) conditions.

Vulnerabilities Details:

- **CVE-2024-20252 and CVE-2024-20254(CVSS score 9.6 Critical) Cisco Expressway Series Cross-Site Request Forgery Vulnerabilities**
- **CVE-2024-20255(CVSS Base Score: 8.2 High) Cisco Expressway Series Cross-Site Request Forgery Vulnerability**
- Cisco Expressway Series devices contain vulnerabilities in their API, allowing unauthenticated remote attackers to conduct Cross-Site Request Forgery (CSRF) attacks. These vulnerabilities arise from insufficient CSRF protection within the affected system's web-based management interface. Attackers can exploit them by tricking API users into clicking malicious links.
- A successful exploit of this vulnerability could allow an attacker to perform arbitrary actions with the privileges of the affected user. This includes modifying the system configuration and creating new privileged accounts, especially if the user has administrative privileges. Additionally, overwriting system configuration settings could prevent the system from processing calls properly, resulting in a denial-of-service (DoS) condition.

Affected Products:

- CVE-2024-20254 and CVE-2024-20255: These vulnerabilities affect Cisco Expressway Series devices in the default configuration.
- CVE-2024-20252: This vulnerability affects Cisco Expressway Series devices if the cluster database (CDB) API feature has been enabled. This feature is disabled by default.

Affected Versions	Fixed Versions
Earlier than 14.0	Migrate to a fixed release.
14	14.3.41
15	15.0.01

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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:

1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3