THREAT ADVISORY

February 12, 2024

Cisco Expressway Gateways (Critical)

SUMMARY

Cisco reported three vulnerabilities impacting its Expressway Series collaboration gateways, with two rated as critical severity and potentially exposing susceptible devices to cross-site request forgery (CSRF) attacks.

RISK SCORING

CVE-ID	CVSSv3 Score
CVE-2024-20252	9.6
CVE-2024-20254	9.6
CVE-2024-20255	8.2

VULNERABILITY DETAILS

CSRF vulnerabilities can be exploited by attackers to deceive authenticated users into unwittingly initiating malicious actions. This includes activities like adding unauthorized user accounts, executing arbitrary code, acquiring administrative privileges, and other unauthorized actions, typically by enticing users to click on malicious links or visit attacker-controlled web pages.

CVE-2024-20252 and CVE-2024-20254:
Unauthenticated attackers can exploit the two critical CSRF vulnerabilities in Expressway gateways to target unpatched devices remotely. CVE-2024-20252 specifically targets gateways where the cluster database (CDB) API feature has been activated, limiting its exploitability to those configurations. By convincing a user to click on a specially crafted link, attackers could execute arbitrary actions with the user's privilege level. If the affected user has administrative privileges, this could result in modifying system configurations and creating new privileged accounts. Note: these vulnerabilities impact Cisco Expressway Series devices in their default configurations.

CVE-2024-20255:
The CSRF security vulnerability can also enable attackers to manipulate the configuration of vulnerable systems and induce denial of service conditions. CVE-2024-20252 specifically targets gateways where the cluster database (CDB) API feature has been activated, limiting its exploitability to those configurations.

AFFECTED PRODUCTS

- Expressway Series: 14.0 and older, 15.0
- Cisco TelePresence Video Communication Server: All versions

SOLUTIONS

- Update to Expressway Series: 14.3.4 and 15.0.0
- Cisco says it will not release security updates for the Cisco TelePresence Video Communication Server (VCS) gateway to address the three vulnerabilities since they have reached the end-of-support date on December 31, 2023.

REFERENCES

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3#fs
- https://www.cybersecurity-help.cz/vdb/SB2024020839
- https://www.bleepingcomputer.com/news/security/critical-cisco-bug-exposes-expressway-gateways-to-csrf-attacks/
- https://bnnbreaking.com/tech/cisco-discloses-three-critical-csrf-vulnerabilities-in-expressway-series