SecurityRisk ADVISORS

Threat Bulletin

Cisco Critical Vulnerabilities

Executive Summary

On June 15, 2022, Cisco released a security advisory that acknowledge two critical vulnerabilities that are currently affecting Cisco's Email Security Appliance and Small Business Routers. There is currently no evidence that these vulnerabilities are being actively exploited in the wild.

The email-based vulnerability relates to improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication. A successful exploit could allow the attacker to gain unauthorized access to the web-based management interface of the affected device.

The router-based vulnerability currently has no available patch and occurs because of insufficient user input validation of incoming HTTP packets. A successful exploit could allow attackers to execute arbitrary commands on an affected device using root-level privileges.

Affected Products

Email-based vulnerability:

- Cisco ESA
- Cisco Secure Email and Web Manager

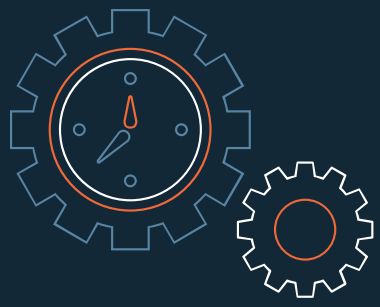
Router-based vulnerability:

- RV110W Wireless-N VPN Firewall
- RV130 VPN Router
- RV130W Wireless-N Multifunction VPN Router
- RV215W Wireless-N VPN Router

Safeguards/Recommendations

Email-based vulnerability:

- Update to the most recent version of AsyncOS software
- If updating is not an option, the workaround is available by disabling the anonymous binds on the external authentication server to prevent exploitation



Vendor: Cisco

CVE-ID: CVE-2022-20798, CVE-2022-20825

Published: 2022 June 15

CVSS V3 Overall Score: 9.8

Criticality: Critical

Patch Availability: See Recommendations

Vulnerability Type: Remote Code Execution, Denial of Service, External Authentication Bypass

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined

Router-based vulnerability:

- There are no currently available patches or workarounds
- Cisco recommends that customers migrate to the Cisco Small Business RV132W, RV160, or RV160W Routers

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-overflow-s2r82P9v

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io