April 24, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco Adaptive Security (ASA) Software – multiple versions and platforms
- Cisco Firepower Threat Defense (FTD) Software – multiple versions and platforms

Technical Details

A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.
This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20353 CVE-2024-20359
- Cyber Activity Impacting CISCO ASA VPNs
- Cisco Security Advisory – cisco-sa-asaftd-websrvs-dos-X8gNucD2
- Cisco Security Advisory – cisco-sa-asaftd-persist-rce-FLsNXF4h
- Cisco Security Advisories