Security Advisory 2024-114

Multiple Critical CISCO Vulnerabilities

2025-10-24 — v1.0

TLP:CLEAR

History:

- *25/10/2024 — v1.0 – Initial publication*

Summary

A set of critical vulnerabilities affecting Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco Secure Firewall Management Center (FMC) Software, and Cisco Nexus Dashboard Fabric Controller (NDFC) have been identified [1-4]. These vulnerabilities can potentially allow attackers to conduct various types of attacks, including command injection, remote command execution, arbitrary command execution, and unauthorised access through static credentials due to improper input validation or insecure handling of web services components. Successful exploitation could allow attackers to execute arbitrary commands, gain root-level access through SSH, or gain unauthorised access via static credentials. They obtained CVSS score of 9 out of 10 or more.

Technical Details

1. **Command Injection Vulnerability**: A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system as root or to execute commands on managed Cisco Firepower Threat Defense (FTD) devices. This vulnerability is due to insufficient input validation of certain HTTP requests. To exploit this vulnerability, the attacker would need valid credentials for a user account with at least the role of Security Analyst (Read Only) [2].
2. **SSH Remote Command Injection Vulnerability**: A vulnerability in the SSH subsystem of Cisco ASA Software could allow an authenticated, remote attacker to execute operating system commands as root. This vulnerability arises from insufficient validation of user input when executing remote CLI commands over SSH. An attacker with limited user privileges could exploit this vulnerability to gain complete control over the system [4].
3. **Arbitrary Command Execution Vulnerability**: A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack. This vulnerability is due to improper user authorisation and insufficient validation of command arguments, allowing attackers to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges. This vulnerability does not affect Cisco NDFC when configured for storage area network (SAN) controller deployment [3].

4. **Static Credential Vulnerability**: A vulnerability in Cisco Firepower Threat Defense (FTD) Software for Firepower 1000, 2100, 3100, and 4200 Series could allow an unauthenticated, local attacker to access an affected system using static credentials. This vulnerability is due to the presence of static accounts with hard-coded passwords on an affected system. Successful exploitation could allow the attacker to access the affected system, retrieve sensitive information, perform limited troubleshooting actions, modify some configuration options, or render the device unbootable [1].

Affected Products

The vulnerabilities affect the following Cisco products:

- Cisco Adaptive Security Appliance (ASA) with CiscoSSH stack enabled and SSH access allowed on a least one interface.
- Cisco Secure Firewall Management Center (FMC) Software.
- Cisco Nexus Dashboard Fabric Controller (NDFC).
- Cisco Firepower Threat Defense (FTD) Software for Firepower 1000, 2100, 3100, and 4200 Series running Cisco FTD Software Release 7.1 through 7.4 with a vulnerability database (VDB) release of 387 or earlier

Recommendations

- **Upgrade to Fixed Software**: Cisco has released software updates to address these vulnerabilities. Ensure all affected Cisco ASA, FMC, FTD, and NDFC devices are upgraded to a fixed release as described on the customer portal.
- **Disable CiscoSSH Stack**: For the SSH remote command injection vulnerability and to determine whether the CiscoSSH stack is enabled on a device, use the `show running-config | include ssh` command and verify the presence of the `ssh stack ciscossh` configuration.
- **Workaround for Static Credential Vulnerability**: Contact Cisco Technical Assistance Center (TAC) to coordinate implementation of the workaround if upgrading to a fixed release is not immediately possible [6]. To determine whether static accounts are present see the detection section of this advisory.

Detection

Static Account Vulnerability

To determine whether static accounts are present, use the `show local-user` command from the security scope in the Cisco FXOS CLI. The following specific accounts are static:

- `csm_processes`
- `report`
- `sftop10user`
- `Sourcefire`
- `SRU`

To detect access to the mentioned accounts has occurred, run the following command from expert mode as the root user. If no output is returned, the vulnerable accounts have not been accessed on the device during the retention period of the logs.

```
zgrep -E "Accepted password for (csm_processes|report|sftop10user|Sourcefire|SRU)" /ngfw/var/log/messages*
```

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF

[4] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr