Security Advisory 2022-051

Cisco Nexus Dashboard Multiple Vulnerabilities

July 22, 2022 — v1.0

TLP:WHITE

History:

- *22/07/2022 — v1.0 – Initial publication*

Summary

On July 20th, Cisco released a security advisory, that addresses one **Critical** and two **High** severity vlnerabilities found in Cisco Nexus Dashboard. The vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary commands, read or upload container image files, or perform a cross-site request forgery attack [1].

Cisco's Product Security Incident Response Team (PSIRT) is not aware of any active exploitation of these vulnerabilities in the wild and the company has released software updates to address these vulnerabilities.

Technical Details

Critical Vulnerability

- **CVE-2022-20857: Cisco Nexus Dashboard Arbitrary Command Execution Vulnerability**

This flaw is due to insufficient access controls and it enables a remote, unauthenticated threat actor to exploit a specific API by sending crafted HTTP requests. This could allow an attacker to execute arbitrary commands with **root privileges** *in any pod on a node*.

High Severity Vulnerabilities

- **CVE-2022-20861: Cisco Nexus Dashboard Cross-Site Request Forgery Vulnerability**

The first high severity bug is due to insufficient CSRF protections for the web UI and can be exploited by persuading an authenticated administrator of the web-based management interface to click a malicious link. A successful exploit could allow a remote attacker to perform actions with **Administrator privileges**.

- **CVE-2022-20858: Cisco Nexus Dashboard Container Image Read and Write Vulnerability**

The second high severity bug enables a remote, unauthenticated threat actor to download container images, or upload malicious ones to an affected device, by opening a TCP connection to the affected service. The malicious images would be run after the device has rebooted or a pod has restarted.

Affected Products

The following products are affected from these vulnerabilities:

- Cisco Nexus Dashboard 1.1 and later

Please note that version 1.1 is not affected by the vulnerability CVE-2022-20858.

Recommendations

Cisco has addressed the vulnerabilities in the 2.2(1e) security update and advises customers to upgrade to an appropriate fixed software release [2].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-mhcvuln-vpsBPJ9y

[2] https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes