April 3, 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 was an update for the following:

- Cisco Nexus Dashboard Fabric Controller (NDFC) – version 12.1.3b

Technical Details

A vulnerability in the Out-of-Band (OOB) Plug and Play (PnP) feature of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an unauthenticated, remote attacker to read arbitrary files.
This vulnerability is due to an unauthenticated provisioning web server. An attacker could exploit this vulnerability through direct web requests to the provisioning server. A successful exploit could allow the attacker to read sensitive files in the PnP container that could facilitate further attacks on the PnP infrastructure.

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-2024-20348 CVE-2024-20334 CVE-2024-20362 CVE-2024-20282 CVE-2024-20302 CVE-2024-20283 CVE-2024-20281 CVE-2024-20332 CVE-2024-20368 CVE-2024-20367 CVE-2024-20310 CVE-2024-20347 CVE-2024-20352 CVE-2024-20306
- Cisco Security Advisory – cisco-sa-ndfc-dir-trav-SSn3AYDw
- Cisco Security Advisories