Advisory Alert

Alert Number: AAA20241003 **Date:** October 3, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Arbitrary Command Execution Vulnerability
Juniper	**High**	Blast-RADIUS Vulnerability
Cisco	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Arbitrary Command Execution Vulnerability (CVE-2024-20432)
Description	Cisco has released security updates addressing an Arbitrary Command Execution Vulnerability that exists in Cisco Nexus Dashboard Fabric Controller. This vulnerability could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco NDFC Release 12.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Blast-RADIUS Vulnerability (CVE-2024-3596)
Description	Juniper has released security updates addressing the Blast-RADIUS Vulnerability that exists in their products. **CVE-2024-3596** - An Authentication Bypass by Spoofing vulnerability in RADIUS protocol of Juniper Networks Junos OS, Junos OS Evolved, Junos OS on cRPD series and other platforms allows an on-path attacker between RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. This vulnerability depends on using the MD5 hash function to pass undetected attribute forgery by modifying RADIUS server Responses (Access-Accept, Access-Reject, or Access-Challenge) Juniper has advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Junos OS • All versions before 21.4R3-S9 • from 22.2 before 22.2R3-S5 • from 22.4 before 22.4R3-S5 • from 23.2 before 23.2R2-S3 • from 23.4 before 23.4R2-S3 • from 24.2 before 24.2R2 Juniper Networks Junos OS Evolved • All versions before 21.4R3-S9-EVO • from 22.2 before 22.2R3-S5-EVO • from 22.3 before 22.3R3-S4-EVO • from 22.4 before 22.4R3-S5-EVO • from 23.2 before 23.2R2-S3-EVO • from 23.4 before 23.4R2-S3-EVO • from 24.2 before 24.2R2-EVO Juniper Networks Junos OS on cRPD • 23.4 version and later versions before 23.4R3-S5 • from 24.2 before 24.2R2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-09-30-Out-of-Cycle-Security-Advisory-Multiple-Products-RADIUS-protocol-susceptible-to-forgery-attacks-Blast-RADIUS-CVE-2024-3596?language=en_US

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20393,CVE-2024-20470,CVE-2024-20449,CVE-2024-20498,CVE-2024-20499,CVE-2024-20500,CVE-2024-20501,CVE-2024-20502,CVE-2024-20513,CVE-2024-20516,CVE-2024-20517,CVE-2024-20518,CVE-2024-20519,CVE-2024-20520,CVE-2024-20521,CVE-2024-20522,CVE-2024-20523,CVE-2024-20524,CVE-2024-20385,CVE-2024-20438,CVE-2024-20441,CVE-2024-20442,CVE-2024-20477,CVE-2024-20490,CVE-2024-20491,CVE-2024-20444,CVE-2024-20448,CVE-2024-20509,CVE-2024-20515,CVE-2024-20492,CVE-2024-20365)
Description	Cisco has released security updates addressing multiple vulnerabilities in that exist in their products. Exploiting these vulnerabilities could lead to Privilege Escalation, Remote Command Execution, Denial of Service, Information Disclosure Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-ptrce-BUSHLbp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv04x_rv32x_vulns-yJ2OSDhV • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-tlsvld-FdUF3cpw • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-idv-Bk8VqEDc • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-raci-T46k3jnN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cidv-XvyX2wLj • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-ZYF2nEEX • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expw-escalation-3bkz77bD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-redfish-cominj-sbkv5ZZ

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security patch updates addressing multiple vulnerabilities in Drupal Modules. Exploiting these vulnerabilities could lead to Access bypass, Information Disclosure Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Diff module versions below 2.0.0-beta3 for Drupal Diff module versions below to 1.8.0 for Drupal Diff module versions 2.0.0 and above for Drupal Two-factor Authentication (TFA) module versions prior to 1.8.0 for Drupal 8+ Two-factor Authentication (TFA) module versions prior to 1.8.0 for Drupal 7 Persistent Login 8.x-1.x module for Drupal Persistent Login 2.x module for Drupal
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-042 • https://www.drupal.org/sa-contrib-2024-043 • https://www.drupal.org/sa-contrib-2024-044

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.