Advisory Alert

Alert Number: **AAA20240523** **Date:** **May 23, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
Drupal	**High**	Multiple Access Bypass Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29469, CVE-2023-28484, CVE-2022-40304, CVE-2022-40303, CVE-2022-40898, CVE-2023-1786, CVE-2022-23491, CVE-2022-4304)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in Dell PowerProtect appliances. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerProtect DD series appliances • DDOS Versions 7.0 through 7.12 • DDOS LTS 2023 7.10 Versions 7.10.1.0 through 7.10.1.15 • DDOS LTS 2022 7.7 Versions 7.7.5.1 through 7.7.5.25 Dell PowerProtect DD Virtual Edition • DDOS Versions 7.0 through 7.12 • DDOS LTS 2023 7.10 Versions 7.10.1.0 through 7.10.1.15 • DDOS LTS 2022 7.7 Versions 7.7.5.1 through 7.7.5.25 Dell APEX Protection Storage • DDOS Versions 7.0 through 7.12 • DDOS LTS 2023 7.10 Versions 7.10.1.0 through 7.10.1.15 • DDOS LTS 2022 7.7 >Versions 7.7.5.1 through 7.7.5.25 PowerProtect DP Series Appliance: All Models Versions prior to 2.7.6 PowerProtect Data Manager Appliance model: DM5500 DDOS Versions prior to 5.15.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223029/dsa-2024-102-security-update-for-dell-technologies-powerprotect-dd-vulnerabilitie

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Access Bypass Vulnerabilities
Description	Drupal has released security updates addressing multiple Access Bypass vulnerabilities that exist in Email Contact and Commerce View Receipt modules. The Email Contact module does not sufficiently handle restricted entity or field access to the mail sending form, when the "Email contact link" formatter is used. The Commerce View Receipts module doesn't sufficiently check access permissions, allowing an unauthorized user to view the private information of other customers. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Email Contact versions prior to 2.0.4 Commerce View Receipt versions prior to 1.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-020 • https://www.drupal.org/sa-contrib-2024-021

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20360, CVE-2024-20293, CVE-2024-20363, CVE-2024-20261, CVE-2024-20361, CVE-2024-20355)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause SQL Injection, Authorization Bypass, Access Control List Bypass, File Policy Bypass, Rule Bypass and ACL Bypass . Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Products running Open Source Snort 3 versions prior to 3.1.69.0 • Cisco FirePOWER Services • Cisco Firepower Threat Defense Software for Cisco Firepower 4200 Series Firewalls Following Products running Cisco IOS XE Software versions prior to 17.12.3 and 17.13.1 • 1000 Series Integrated Services Routers (ISRs) • 4000 Series ISRs • Catalyst 8000V Edge Software • Catalyst 8200 Series Edge Platforms • Catalyst 8300 Series Edge Platforms • Catalyst 8500L Edge Platforms • Cloud Services Routers 1000V • Integrated Services Virtual Router (ISRv) Cisco Firepower Management Center (Use Cisco Software Checker to identify vulnerable version)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs#fs • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-ips-bypass-uE69KBMd • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-archive-bypass-z4wQjwcN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-object-bypass-fTH8tDjq • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-saml-bypass-KkNvXyKW

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.