Advisory Alert

Alert Number: AAA20241205 **Date:** December 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Image Verification Bypass Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34048, CVE-2023-34056)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell PowerStore. **CVE-2023-34048** - vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution. **CVE-2023-34056** - vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	vCenter Versions prior to 7.0U3o of following products PowerStore 1000X PowerStore 3000X PowerStore 5000X PowerStore 7000X PowerStore 9000X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219749/dsa-2023-433-dell-powerstore-security-update-for-vmware-vulnerabilities

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Image Verification Bypass Vulnerability (CVE-2024-20397)
Description	Cisco has released security updates addressing an Image Verification Bypass Vulnerability that exists in Cisco NX-OS Software. This vulnerability is due to insecure bootloader settings. An attacker could exploit this vulnerability by executing a series of bootloader commands. A successful exploit could allow the attacker to bypass NX-OS image signature verification and load unverified software. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Cisco products if they are running on a vulnerable version of Cisco NX-OS Software MDS 9000 Series Multilayer Switches Nexus 3000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Fabric Switches in ACI mode Nexus 9000 Series Switches in standalone NX-OS mode UCS 6400 Series Fabric Interconnects UCS 6500 Series Fabric Interconnects
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43102, CVE-2024-38477, CVE-2024-38474, CVE-2024-38475, CVE-2024-38473, CVE-2024-39573, CVE-2024-28849, CVE-2023-49582, CVE-2024-49602, CVE-2024-49603, CVE-2024-42426)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell PowerScale OneFS. 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	PowerScale OneFS Versions 8.2.2.x through 9.7.1.2 and Versions 9.8.0.0 through 9.9.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000256645/dsa-2024-453-security-update-for-dell-powerscale-onefs-multiple-security-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35949, CVE-2024-43861)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory leak and out-of-bound access. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20244170-1/

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting, Cross Site Request Forgery and Access Bypass. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Entity Form Steps module versions prior to 1.1.4 for Drupal 9.x/10.x • Minify JS module versions prior to 3.0.3 • Download All Files module versions prior to 2.0.2 • Pages Restriction Access module versions prior to 2.0.3 for Drupal 8.x or higher • OAuth & OpenID Connect Single Sign On - SSO (OAuth/OIDC Client) versions prior to 8.x-3.44 for Drupal 9 and Drupal 10 • OAuth & OpenID Connect Single Sign On - SSO (OAuth/OIDC Client) versions prior to 4.0.19 for Drupal 9, Drupal 10 and Drupal 11 • OAuth & OpenID Connect Single Sign On - SSO (OAuth/OIDC Client) versions prior to 1.355 for Drupal 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-071 • https://www.drupal.org/sa-contrib-2024-070 • https://www.drupal.org/sa-contrib-2024-069 • https://www.drupal.org/sa-contrib-2024-068 • https://www.drupal.org/sa-contrib-2024-067

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.