Advisory Alert

Alert Number: **AAA20240429** **Date:** **April 29, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Remote Code Execution Vulnerabilities
Drupal	**Critical**	Access Bypass Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
QNAP	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Remote Code Execution Vulnerabilities (CVE-2021-44228, CVE-2021-45046)
Description	Dell has issued security updates addressing multiple Remote Code Execution vulnerabilities that exist in Dell Integrated Data Protection Appliance. 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 Integrated Data Protection Appliance versions 2.7.1 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000194532/dsa-2021-285-dell-emc-integrated-data-protection-appliance-powerprotect-dp-series-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has issued security updates addressing an Access Bypass Vulnerability that exists in Advanced PWA components. This module doesn't sufficiently protect access to the settings form, allowing an unauthorized malicious user to view and modify the module settings. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Advanced Progressive Web App 8.x versions prior to 1.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-017

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. If Exploited, these vulnerabilities could lead to Denial of Service, Privilege Escalation, Information Disclosure, Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241454-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. 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	Unisphere for PowerMax - Host Installation versions prior to 9.2.4.7 Unisphere for PowerMax - Virtual Appliance versions prior to 9.2.4.7 Unisphere 360 - Host Installation versions prior to 9.2.4.11 Solutions Enabler Virtual Appliance versions prior to 9.2.4.5 Dell PowerMax EEM - Embedded Management version 5978 PowerMaxOS 5978 version 5978 Dell OpenManage Enterprise versions 4.0.0 and 4.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000220427/dsa-2023-443-dell-powermaxos-5978-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224251/dsa-2024-184-security-update-for-dell-openmanage-enterprise-vulnerability

Affected Product	**QNAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51364, CVE-2023-51365, CVE-2024-21905, CVE-2023-50361, CVE-2023-50362, CVE-2023-50363, CVE-2023-50364 CVE-2023-5824, CVE-2023-46724, CVE-2023-46846, CVE-2023-46847)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive Information Disclosure, Code Execution, Authentication Bypass. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.1.x QTS 4.5.x QuTS hero h5.1.x QuTS hero h4.5.x QuTScloud c5.x Proxy Server 1.4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-24-14 • https://www.qnap.com/en/security-advisory/qsa-24-16 • https://www.qnap.com/en/security-advisory/qsa-24-20 • https://www.qnap.com/en/security-advisory/qsa-24-18

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability
Description	Drupal has released security updates addressing an Information Disclosure Vulnerability that exists in REST Views module. Paths to unpublished entities (such as nodes) will be exposed if those entities are referenced from other entities listed in a REST display, and the reference field on those listed entities is displayed with the "Entity path" formatter. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	REST Views 2.x versions REST Views 3.x versions prior to 3.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-018

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.