



Advisory Alert

Alert Number: AAA20231018

Date: October 18, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Critical	Multiple Vulnerabilities
Oracle	Critical	Multiple Vulnerabilities
Suse	High	Multiple Vulnerabilities
Juniper	High	Improper Exception Handling Vulnerability
Ubuntu	High, Medium, Low	Multiple Vulnerabilities
HPE	Medium	Authenticated Sensitive Information Disclosure Vulnerability

Description

Affected Product	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	<p>Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Successful exploitation of these vulnerabilities could lead to multiple flaws.</p> <p>Dell strongly recommends to apply the necessary security updates at earliest to avoid issues</p>
Affected Products	Dell Unity Operating Environment (OE) Versions prior to 5.3.1 PowerProtect DD DDOS, DDMC, and SmartScale 7.0 to 7.11 PowerProtect DD DDOS, DDMC, and SmartScale 6.2.1.100 and below PowerProtect DD DDOS, DDMC 6.2.1.100 and below Dell Object Scale Versions 1.0.0, 1.0.1, 1.0.2, and 1.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218604/dsa-2023-349-security-update-for-dell-unity-family-dell-emc-unity-all-flash-for-multiple-component-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000218619/dsa-2023-389-security-update-for-dell-technologies-powerprotect-datadomain-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000218660/dsa-2023-381-security-update-for-dell-objectscale-1-3-vulnerabilities

Affected Product	Oracle
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	<p>Oracle has released October 2023 Security Updates addressing vulnerabilities in Oracle code and in third-party components included in Oracle products.</p> <p>Oracle strongly recommends to apply necessary security patches at earliest to avoid issues</p>
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuoct2023.html

Affected Product	Suse
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36766, CVE-2023-1192, CVE-2023-1206, CVE-2023-1859, CVE-2023-2177, CVE-2023-23454, CVE-2023-4004, CVE-2023-40283, CVE-2023-42753, CVE-2023-4389, CVE-2023-4622, CVE-2023-4623, CVE-2023-4881, CVE-2023-4921, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-4155, CVE-2023-42754, CVE-2023-4563, CVE-2023-4921, CVE-2023-5345)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to Privilege escalation, Denial of service, Potential information disclosure, Stack overflow Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 15-SP3, 15-SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2 SUSE Real Time Module 15-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234095-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234093-1/

Affected Product	Juniper
Severity	High
Affected Vulnerability	Improper Exception Handling Vulnerability (CVE-2023-44186)
Description	Juniper has released a security update addressing an Improper Exception Handling vulnerability affecting Juniper Networks Junos OS and Junos OS Evolved. Exploitation of this vulnerability could an attacker to send a BGP update message with an AS PATH containing a large number of 4-byte ASes, leading to a Denial of Service (DoS). Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Networks Junos OS: All versions prior to 20.4R3-S8; 21.1 versions 21.1R1 and later; 21.2 versions prior to 21.2R3-S6; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S5; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.2 versions prior to 23.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S8-EVO; 21.1 versions 21.1R1-EVO and later; 21.2 versions prior to 21.2R3-S6-EVO; 21.3 versions prior to 21.3R3-S5-EVO; 21.4 versions prior to 21.4R3-S5-EVO; 22.1 versions prior to 22.1R3-S4-EVO; 22.2 versions prior to 22.2R3-S2-EVO; 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO; 23.2 versions prior to 23.2R2-EVO.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-attempting-to-send-a-very-long-AS-PATH-to-a-non-4-byte-AS-capable-BGP-neighbor-CVE-2023-44186?language=en_US

Affected Product	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27672, CVE-2023-4128, CVE-2023-40283, CVE-2023-3212, CVE-2023-3863, CVE-2022-40982)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to sensitive Information disclosure, denial of service, arbitrary code execution Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6396-3

Affected Product	HPE
Severity	Medium
Affected Vulnerability	Authenticated Sensitive Information Disclosure Vulnerability (CVE-2023-4896)
Description	HPE has released a security update addressing an Authenticated Sensitive Information Disclosure Vulnerability that exist in their products. Successful exploitation could allow an attacker to gain access to some data that could be further exploited to laterally access devices managed and monitored by the AirWave server. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE Aruba Networking AirWave Management Platform <ul style="list-style-type: none"> • 8.3.0.1 and below • 8.2.15.2 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04546en_us

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.