Advisory Alert

Alert Number: **AAA20230606** **Date:** **June 6, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42003, CVE-2022-42004, CVE-2021-22569, CVE-2022-3171, CVE-2021-37533, CVE-2022-23471, CVE-2023-25153, CVE-2023-25173, CVE-2023-27561, CVE-2022-46146, CVE-2022-1705, CVE-2022-1962, CVE-2022-24675, CVE-2022-27664, CVE-2022-28131, CVE-2022-28327, CVE-2022-2879, CVE-2022-2880, CVE-2022-30580, CVE-2022-30630, CVE-2022-30631, CVE-2022-30632, CVE-2022-30633, CVE-2022-30635, CVE-2022-32148, CVE-2022-32189, CVE-2022-32190, CVE-2022-41715, CVE-2022-41716, CVE-2022-41717, CVE-2022-41723, CVE-2022-41724, CVE-2022-41725, CVE-2023-24532, CVE-2021-43565, CVE-2022-27191, CVE-2022-41721, CVE-2022-29526)
Description	Dell has released a security update addressing multiple Critical vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could cause Access Bypass, Privilege Escalation, Denial of Service and Sensitive information disclosure. Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Dell Streaming Data Platform Versions 1.1.x through 1.6.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000214599/dsa-2023-195-dell-streaming-data-platform-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2006-20001, CVE-2022-25147, CVE-2022-43551, CVE-2022-43552, CVE-2022-43680, CVE-2023-23914, CVE-2023-23915, CVE-2023-23916, CVE-2023-25690, CVE-2022-3564, CVE-2022-4378)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Use-after-free condition, HSTS bypass, Denial of Service, Out-of-bounds read/write. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	JBoss Enterprise Web Server 5 for RHEL 7 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3421 https://access.redhat.com/errata/RHSA-2023:3420 https://access.redhat.com/errata/RHSA-2023:3355 https://access.redhat.com/errata/RHSA-2023:3354 https://access.redhat.com/errata/RHSA-2023:3431

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1281 , CVE-2023-1989 , CVE-2023-2162 , CVE-2023-23454 , CVE-2023-28464, CVE-2023-0386 , CVE-2023-0461)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege escalation, Use-after-free condition and type-confusion in the CBQ network scheduler. Suse recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP1 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP1 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232376-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232371-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232369-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232368-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232367-1/

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.