TLP: WHITE

Advisory Alert

Alert Number: AAA20230719 **Date:** July 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released July 2023 Security Updates addressing vulnerabilities in Oracle code and in third-party components included in Oracle products. Oracle highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujul2023.html

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released critical security updates addressing multiple vulnerabilities affecting their Products. Exploitation of the most severe vulnerabilities may cause Integer overflow, Arbitrary code execution, Remote code execution and NULL pointer deference. Dell highly recommends applying necessary fixes to avoid issues.
Affected Products	Products running PowerStoreT OS Versions prior to 3.5.0.1-2083289 • PowerStore 500T • PowerStore 1000T • PowerStore 1200T • PowerStore 3000T • PowerStore 3200T • PowerStore 5000T • PowerStore 5200T • PowerStore 7000T • PowerStore 9000T • PowerStore 9200T XtremIO X2 All prior releases prior to 6.4.1-11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215905/dsa-2023-248-dell-powerstore-family-security-update-for-multiple-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000215898/dsa-2023-242-security-update-for-dell-xtremio-x2

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3519, CVE-2023-3466, CVE-2023-3467)
Description	Citrix has released a critical security update addressing multiple vulnerabilities affecting Citrix ADC and Citrix Gateway. Exploitation of the most severe vulnerabilities could cause Reflected Cross-Site Scripting (XSS), Privilege Escalation to root administrator (nsroot), Unauthenticated remote code execution Citrix highly recommends applying necessary fixes to avoid issues.
Affected Products	Citrix ADC and Citrix Gateway
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3564, CVE-2023-0461, CVE-2023-1281, CVE-2023-1390, CVE-2023-32233, CVE-2022-1016, CVE-2022-42703, CVE-2022-42896, CVE-2023-2002, CVE-2023-2124, CVE-2023-2235, CVE-2023-20883)
Description	Redhat has released patch updates to address multiple flaws that exist in their products. Successful exploitation of these vulnerabilities could cause Denial of service, Privilege escalation, Use-after-free condition, Unauthorized command execution. Redhat highly recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat JBoss Middleware 1 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4151 https://access.redhat.com/errata/RHSA-2023:4150 https://access.redhat.com/errata/RHSA-2023:4146 https://access.redhat.com/errata/RHSA-2023:4145 https://access.redhat.com/errata/RHSA-2023:4138 https://access.redhat.com/errata/RHSA-2023:4137 https://access.redhat.com/errata/RHSA-2023:4130 https://access.redhat.com/errata/RHSA-2023:4126 https://access.redhat.com/errata/RHSA-2023:4125 https://access.redhat.com/errata/RHSA-2023:4200

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36280, CVE-2022-38096, CVE-2022-4269, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2022-4744, CVE-2023-0045, CVE-2023-0122, CVE-2023-0179, CVE-2023-0394, CVE-2023-0461, CVE-2023-0469, CVE-2023-0590, CVE-2023-0597, CVE-2023-1075, CVE-2023-1076, CVE-2023-1077, CVE-2023-1079, CVE-2023-1095, CVE-2023-1118, CVE-2023-1249, CVE-2023-1382, CVE-2023-1513, CVE-2023-1582, CVE-2023-1583, CVE-2023-1611, CVE-2023-1637, CVE-2023-1652, CVE-2023-1670, CVE-2023-1829, CVE-2023-1838, CVE-2023-1855, CVE-2023-1989, CVE-2023-1998, CVE-2023-2002, CVE-2023-21102, CVE-2023-21106, CVE-2023-2124, CVE-2023-2156, CVE-2023-2162, CVE-2023-2176, CVE-2023-2235, CVE-2023-2269, CVE-2023-22998, CVE-2023-23000, CVE-2023-23001, CVE-2023-23004, CVE-2023-23006, CVE-2023-2430, CVE-2023-2483, CVE-2023-25012, CVE-2023-2513, CVE-2023-26545, CVE-2023-28327, CVE-2023-28410, CVE-2023-28464, CVE-2023-28866, CVE-2023-3006, CVE-2023-30456, CVE-2023-30772, CVE-2023-3090, CVE-2023-31084, CVE-2023-3111, CVE-2023-3141, CVE-2023-31436, CVE-2023-3161, CVE-2023-3212, CVE-2023-3220, CVE-2023-32233, CVE-2023-33288, CVE-2023-3357, CVE-2023-3358, CVE-2023-3389, CVE-2023-33951, CVE-2023-33952, CVE-2023-35788, CVE-2023-35823, CVE-2023-35828, CVE-2023-35829)
Description	Suse has released a security update addressing multiple vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could lead to Heap out-of-bounds write, Use-after-free flaw, NULL pointer dereference. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232871-1/

Affected Product	**IBM**
Severity	**High** ,**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27554, CVE-2023-30447, CVE-2023-30446, CVE-2023-30443, CVE-2023-30448, CVE-2023-30445, CVE-2023-30449, CVE-2023-23487, CVE-2023-30431, CVE-2023-27869, CVE-2023-27867, CVE-2023-27868, CVE-2023-30442, CVE-2023-29256, CVE-2023-27558, CVE-2023-35012)
Description	IBM has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead Sensitive information disclosure, Denial of Service, Arbitrary code execution, Privilege escalation. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0, 8.5 IBM WebSphere Remote Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6989451 https://www.ibm.com/support/pages/node/7012979

Affected Product	**Ubuntu**
Severity	**High** ,**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35788, CVE-2023-0459, CVE-2023-2176, CVE-2023-0597, CVE-2023-2124, CVE-2023-2430, CVE-2023-1073, CVE-2022-4842)
Description	Ubuntu has released security updates addressing Multiple Vulnerabilities within their products. If exploited theses vulnerabilities could lead to Arbitrary code execution, Sensitive Information disclosure, Denial of service. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6234-1 https://ubuntu.com/security/notices/USN-6235-1

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.