Advisory Alert

Alert Number: AAA20230419 **Date:** April 19, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released April 2023 Security Updates addressing vulnerabilities in Oracle code and in third-party components included in Oracle products. Oracle strongly recommends to apply necessary security patches at 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/cpuapr2023.html

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28772, CVE-2023-28466 , CVE-2023-28466, CVE-2023-28464 , CVE-2023-28328 , CVE-2023-28327 , CVE-2023-23455 , CVE-2023-23001 , CVE-2023-1838 , CVE-2023-1838, CVE-2023-1652 , CVE-2023-1637 , CVE-2023-1611 , CVE-2023-1582 , CVE-2023-1513 , CVE-2023-1390 , CVE-2023-1382 , CVE-2023-1281 , CVE-2023-1095 , CVE-2023-1078 , CVE-2023-1076 , CVE-2023-1075 , CVE-2023-0461 , CVE-2023-0394 , CVE-2022-4744 , CVE-2022-20567 , CVE-2021-3923 , CVE-2020-36691 , CVE-2017-5753)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities can lead to Denial of Service, Privilege Escalation, Unauthorized access, use-after-free or NULL pointer dereference Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap 15.4 openSUSE Leap Micro 5.3 Public Cloud Module 15-SP4 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4 SUSE Linux Enterprise Live Patching 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 12 SP5, 15 SP3, 15 SP4 SUSE Linux Enterprise Server 12 SP5, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Real Time Module 15-SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231897-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231895-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231894-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231892-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24998, CVE-2022-40664, CVE-2022-27664, CVE-2022-41723, CVE-2022-32149)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could cause Denial of Service and Access bypass. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM Case Manager 5.3.x WebSphere Service Registry and Repository 8.5.0 through to 8.5.6.3 Db2 Rest 1.0.0.121-amd and 64-1.0.0.254-amd64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6984675 https://www.ibm.com/support/pages/node/6962169 https://www.ibm.com/support/pages/node/6984413

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4378, CVE-2023-1017, CVE-2023-1018, CVE-2022-1278, CVE-2022-3509, CVE-2022-3510)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Privilege escalation, Arbitrary code execution, Sensitive information disclosure, Denial of service. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.6 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x 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 - Extended Life Cycle Support (for IBM z Systems) 6 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1822 https://access.redhat.com/errata/RHSA-2023:1833 https://access.redhat.com/errata/RHSA-2023:1855

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26606, CVE-2023-26545, CVE-2023-22997, CVE-2023-1652, CVE-2023-1281, CVE-2023-1074, CVE-2023-1073, CVE-2023-1032, CVE-2023-0468, CVE-2023-0394, CVE-2023-0386, CVE-2022-4842, CVE-2022-47929, CVE-2022-4129, CVE-2022-41218, CVE-2022-3424)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 22.10 Ubuntu 22.04 LTS Ubuntu 22.04 Ubuntu 20.04 LTS Ubuntu 20.04 Ubuntu 18.04 LTS Ubuntu 16.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6025-1 https://ubuntu.com/security/notices/USN-6024-1 https://ubuntu.com/security/notices/LSN-0094-1

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.