Advisory Alert

Alert Number: AAA20241016 **Date:** October 16, 2024

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**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle 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. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuoct2024.html

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Integer Overflow, Use After Free, Double Free, Memory Corruption, Race condition, False Positive Lockdep. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP2, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243624-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243625-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243626-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243627-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243628-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243631-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243632-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243635-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243636-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243638-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243639-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243640-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243641-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243642-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7254, CVE-2024-45085, CVE-2024-26643, CVE-2024-27397, CVE-2024-22354, CVE-2023-6240, CVE-2023-52667, CVE-2024-33601, CVE-2024-22329, CVE-2023-52675, CVE-2024-26659, CVE-2024-26735, CVE-2024-25026, CVE-2024-26602, CVE-2024-33599, CVE-2023-52686, CVE-2024-36004, CVE-2023-52835, CVE-2024-26585, CVE-2024-33602, CVE-2024-26993, CVE-2024-33600, CVE-2024-6387, CVE-2024-26583, CVE-2024-26584, CVE-2023-4244, CVE-2024-0443, CVE-2024-26804, CVE-2024-26808, CVE-2024-2961)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, Privilege Escalation, Server-side Request Forgery (SSRF), Buffer Overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty - Versions 20.0.0.12 - 24.0.0.10 IBM WebSphere Application Server IBM Storage Scale System 8.5 IBM Storage Scale System - Versions 6.1.0.0-6.1.9.3, 6.2.0.0-6.2.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173097 • https://www.ibm.com/support/pages/node/7173128 • https://www.ibm.com/support/pages/node/7173184

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38602, CVE-2024-38621, CVE-2024-42223, CVE-2024-41097, CVE-2024-42284, CVE-2024-27051, CVE-2024-38627,CVE-2024-39487, CVE-2023-52528, CVE-2024-42280, CVE-2024-38611, CVE-2024-42089, CVE-2024-31076, CVE-2024-36971, CVE-2024-43858, CVE-2024-42157, CVE-2024-45016, CVE-2024-42271, CVE-2024-26754, CVE-2024-26641, CVE-2024-27436, CVE-2024-40901, CVE-2024-39494, CVE-2024-26810, CVE-2024-26602, CVE-2024-26812, CVE-2024-42229 , CVE-2024-42244, CVE-2024-41073, CVE-2023-52510, CVE-2024-40941, CVE-2024-46673, CVE-2024-44940, CVE-2024-26960, CVE-2024-38630)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04 ESM Ubuntu 16.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7069-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47385, CVE-2023-28746, CVE-2024-36244, CVE-2024-39472, CVE-2024-41056, CVE-2024-41066, CVE-2024-42090, CVE-2024-42272, CVE-2024-42284, CVE-2021-47560, CVE-2024-26598, CVE-2024-26830, CVE-2024-35884, CVE-2023-52658, CVE-2024-27403, CVE-2024-35989, CVE-2024-36889, CVE-2024-36978, CVE-2024-38556, CVE-2024-39483, CVE-2024-39502, CVE-2024-40959, CVE-2024-42079)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause NULL Pointer Dereference, Information Disclosure, Use After Free. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 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 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64, AUS 9.2 x86_64, AUS 9.4 x86_64, TUS 8.6 x86_64 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 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:8157 • https://access.redhat.com/errata/RHSA-2024:8158 • https://access.redhat.com/errata/RHSA-2024:8161 • https://access.redhat.com/errata/RHSA-2024:8162

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-10768, CVE-2023-26116, CVE-2023-26117,CVE-2023-26118, CVE-2019-14863, CVE-2022-25869)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Cross-site Scripting, JavaScript engine to hang. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) - Versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000141463 • https://my.f5.com/manage/s/article/K000141459

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.