FINCSIRT

Advisory Alert

Alert Number: **AAA20240717** **Date:** **July 17, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ivanti	**High**	SQL-injection vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47548, CVE-2021-47596, CVE-2022-48627, CVE-2023-52638, CVE-2024-26783, CVE-2024-26858, CVE-2024-27397, CVE-2024-27435, CVE-2024-35958, CVE-2024-36270, CVE-2024-36886, CVE-2024-36904, CVE-2024-36957, CVE-2024-38543, CVE-2024-38586, CVE-2024-38593, CVE-2024-38663)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in Linux kernel. These vulnerabilities could be exploited by malicious users to cause use after free condition, NULL pointer dereferences, privilege escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x 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 Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:4583

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party components which affect Dell SmartFabric OS.These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell SmartFabric OS10 versions 10.5.3.9, 10.5.5.9, 10.5.4.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226960/dsa-2024-317-security-update-for-dell-os10-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226956/dsa-2024-315-security-update-for-dell-os10-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226958/dsa-2024-316-security-update-for-dell-os10-third-party-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47145, CVE-2021-47201, CVE-2021-47275, CVE-2021-47438, CVE-2021-47498, CVE-2021-47520, CVE-2021-47547, CVE-2021-47555, CVE-2021-47571, CVE-2023-24023, CVE-2023-4244, CVE-2023-52507, CVE-2023-52670, CVE-2023-52683, CVE-2023-52693, CVE-2023-52752, CVE-2023-52753, CVE-2023-52817, CVE-2023-52818, CVE-2023-52819, CVE-2023-52837, CVE-2023-52846, CVE-2023-52881, CVE-2024-23307, CVE-2024-26635, CVE-2024-26636, CVE-2024-26745, CVE-2024-26828, CVE-2024-26880, CVE-2024-26923, CVE-2024-26930, CVE-2024-35789, CVE-2024-35805, CVE-2024-35819, CVE-2024-35828, CVE-2024-35861, CVE-2024-35862, CVE-2024-35864, CVE-2024-35869, CVE-2024-35947, CVE-2024-35950, CVE-2024-36014, CVE-2024-36894, CVE-2024-36899, CVE-2024-36904, CVE-2024-36940, CVE-2024-36941, CVE-2024-36964, CVE-2024-36971, CVE-2024-38541, CVE-2024-38545, CVE-2024-38559, CVE-2024-38560, CVE-2024-38564, CVE-2024-38578, CVE-2024-38598, CVE-2024-38619, CVE-2024-39301, CVE-2024-39475)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242480-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242487-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242488-1

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-37381)
Description	Ivanti has released a security update addressing an unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2024 flat. **CVE-2024-37381** - An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2024 flat allows an authenticated attacker within the same network to execute arbitrary code. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti EPM 2024 flat
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-July-2024-for-EPM-2024?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-2511, CVE-2024-0727, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2023-33850)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Denial of service, Sensitive information and cause high confidentiality and integrity impact. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM AIX versions 7.2 and 7.3 IBM VIOS versions 3.1 and 4.1 IBM Storage Protect Server 8.1.0.000 - 8.1.22.xxx IBM Storage Protect Operations Center 8.1.0.000 - 8.1.22.xxx
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7160457 • https://www.ibm.com/support/pages/node/7160375 • https://www.ibm.com/support/pages/node/7160374

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. If exploited, these vulnerabilities could lead to denial of service, server-side memory leak, memory overlapping, NULL pointer dereference. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6896-2 • https://ubuntu.com/security/notices/USN-6893-2

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.