TLP: WHITE

Advisory Alert

Alert Number: AAA20250219 **Date:** February 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple TOCTOU Race Condition Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Citrix	**High**, Medium	Multiple Privilege escalation Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
HPE	Medium	Information Disclosure Vulnerability
Joomla	Low	SQL injection vulnerability
FortiGuard	Low	Out-of-bounds Write Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple TOCTOU Race Condition Vulnerabilities (CVE-2024-50379, CVE-2024-56337)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-50379 -** Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration). This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0.M1 through 9.0.97. Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue. **CVE-2024-56337 -** A TOCTOU race condition vulnerability affects Apache Tomcat versions 11.0.0-M1 to 11.0.1, 10.1.0-M1 to 10.1.33, and 9.0.0.M1 to 9.0.97 due to incomplete mitigation of CVE-2024-50379. On case-insensitive file systems with the default servlet write enabled, users may need additional configuration depending on their Java version. Java 8 and 11 require explicitly setting sun.io.useCanonCaches=false, while Java 17 must not override its default false setting. Java 21 and later are unaffected. Tomcat 11.0.3, 10.1.35, and 9.0.99 will enforce proper configuration and disable the cache where possible. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Version(s) - 7.5 - 7.5.0 UP11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7183584

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing Multiple Linux Kernel Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Out-of-bound read, Use-after-free, Races condition, Memory leak, NULL pointer dereference. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Availability Extension 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP4 LTSS, 15 SP5, 15 SP5 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4, 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/2025/suse-su-20250576-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250577-1/

Affected Product	**Citrix**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Privilege escalation Vulnerabilities (CVE-2024-12284, CVE-2025-1222, CVE-2025-1223)
Description	Citrix has released security updates addressing Multiple Vulnerabilities that exist in their products. If exploited an attacker can gain application privileges in order to perform limited modification and/or read arbitrary data Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetScaler Console 14.1-38.53 and Prior releases NetScaler Console 13.1-56.18 and Prior releases of 13.1 NetScaler Agent 14.1-38.53 and Prior releases NetScaler Agent 13.1-56.18 and Prior releases of 13.1 Citrix Secure Access Client for Mac 25.01.2 and Prior releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/s/article/CTX692579-netscaler-console-and-netscaler-agent-security-bulletin-for-cve202412284?language=en_US • https://support.citrix.com/s/article/CTX692679-citrix-secure-access-client-for-mac-security-bulletin-for-cve20251222-and-cve20251223?language=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-51127, CVE-2023-52679, CVE-2024-23307, CVE-2024-26924, CVE-2024-26960, CVE-2024-27011, CVE-2024-27012, CVE-2024-27017, CVE-2024-35824, CVE-2024-35876, CVE-2024-36954, CVE-2024-46695, CVE-2024-50110, CVE-2024-50142, CVE-2024-50256, CVE-2024-50275, CVE-2024-53113, CVE-2023-52490, CVE-2024-53104)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Integer Overflow, system crash, Information Disclosure and Alter System Memory. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64, 8 x86_64, 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 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 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 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 9.4 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 9.4 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 9.4 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 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 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 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 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 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:1635 • https://access.redhat.com/errata/RHSA-2025:1636 • https://access.redhat.com/errata/RHSA-2025:1637 • https://access.redhat.com/errata/RHSA-2025:1638 • https://access.redhat.com/errata/RHSA-2025:1658 • https://access.redhat.com/errata/RHSA-2025:1659 • https://access.redhat.com/errata/RHSA-2025:1662 • https://access.redhat.com/errata/RHSA-2025:1663

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21235, CVE-2024-21217, CVE-2024-21210, CVE-2024-21208, CVE-2024-10917, CVE-2023-37920, CVE-2024-1488, CVE-2024-8508, CVE-2024-12085, CVE-2024-56326, CVE-2018-12699, CVE-2024-35195, CVE-2024-9823, CVE-2024-52337)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Integer Overflow, Information Disclosure, Privilege escalation, Memory leak. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Version(s) - 7.5 - 7.5.0 UP11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7183584

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28047, CVE-2024-39279, CVE-2024-31157)
Description	HPE has released security updates addressing an Information Disclosure Vulnerability that exists in their products. **CVE-2024-28047 -** Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. **CVE-2024-39279 -** Insufficient granularity of access control in UEFI firmware in some Intel(R) processors may allow a authenticated user to potentially enable denial of service via local access. **CVE-2024-31157 -** Improper initialization in UEFI firmware OutOfBandXML module in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE Alletra 4110 - Prior to v2.44_01-17-2025, v2.44_01-17-2025, • HPE Alletra 4140 - Prior to v2.44_01-17-2025 • HPE Apollo 2000 Gen10 Plus System - Prior to v2.30_01-16-2025 • HPE Apollo 2000 System - Prior to v3.40_01-16-2025 • HPE Apollo 4200 Gen10 Plus System - Prior to v2.30_01-16-2025 • HPE Apollo 4200 Gen10 Server - Prior to v3.40_01-16-2025 • HPE Compute Edge Server e930t - Prior to v2.44_01-17-2025 • HPE Edgeline e920 Server Blade - Prior to v2.30_01-16-2025 • HPE Edgeline e920d Server Blade - Prior to v2.30_01-16-2025 • HPE Edgeline e920t Server Blade - Prior to v2.30_01-16-2025 • HPE Synergy 480 Gen10 Compute Module - Prior to v3.40_01-16-2025 • HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.30_01-16-2025 • HPE Synergy 480 Gen11 Compute Module - Prior to v2.44_01-17-2025 • HPE Synergy 660 Gen10 Compute Module - Prior to v3.40_01-16-2025 • HPE ProLiant Gen11 Servers (DL110, DL320, DL360, DL380, DL380a, DL560, ML110, ML350) – Prior to v2.44_01-17-2025 • HPE ProLiant Gen10 Plus Servers (DL110, DL360, DL380, XL220n, XL290n) – Prior to v2.30_01-16-2025 • HPE ProLiant Gen10 Servers (BL460c, DL120, DL160, DL180, DL360, DL380, DL560, DL580, ML110, ML350, XL170r, XL190r, e910, e910t) – Prior to v3.40_01-16-2025 • HPE ProLiant MicroServer Gen10 – Prior to v3.50_01-16-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04790en_us&docLocale=en_US

Affected Product	**Joomla**
Severity	**Low**
Affected Vulnerability	SQL injection vulnerability (CVE-2025-22207)
Description	Joomla has released security updates addressing an SQL injection vulnerability that exists in their products. **CVE-2025-22207 -** Improperly built order clauses lead to a SQL injection vulnerability in the backend task list of com_scheduler Joomla advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Joomla CMS versions 4.0.0-4.4.10, 5.1.0-5.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/958-20250201-core-sql-injection-vulnerability-in-scheduled-tasks-component.html

Affected Product	**FortiGuard**
Severity	**Low**
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2024-52963)
Description	FortiGuard has released security updates addressing an Out-of-bounds Write Vulnerability that exists in their products. **CVE-2024-52963 -** An Out-of-bounds Write in FortiOS IPSEC daemon may allow an unauthenticated attacker to perform a denial of service under certains conditions that are outside the control of the attacker. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.6 - 7.6.0 FortiOS 7.4 - 7.4.0 through 7.4.7 FortiOS 7.2 - 7.2.0 through 7.2.10 FortiOS 7.0 - 7.0 all versions FortiOS 6.4 - 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-373

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.