Advisory Alert

Alert Number: AAA20240809 **Date:** August 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Buffer Overflow Vulnerability
PostgreSQL	**High**	TOCTOU Race Condition Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	SSH Terrapin Vulnerability
F5	**Medium**	Multiple Vulnerabilities
Juniper	**Medium**	Unchecked Return Value Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2024-41660)
Description	IBM has released security updates addressing a Buffer Overflow Vulnerability that exists in IBM Power Systems. **CVE-2024-41660** - OpenBMC slpd-lite is vulnerable to a buffer overflow, caused by improper bounds checking by the the slpd-lite daemon. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Power Systems AC922 (8335-GTG), AC922 (8335-GTH, 8335-GTX) using: • OPENBMC versions OP910.00 - OP910.80 • OPENBMC versions OP940.00 - OP940.60 IBM Power Systems S1022 (9105-22A), S1024 (9105-42A), S1022s (9105-22B), S1014 (9105-41B), L1022 (9786-22H), L1024 (9786-42H) using: • OPENBMC versions FW1020.00 - FW1020.60 • OPENBMC versions FW1030.00 - FW1030.50 • OPENBMC versions FW1050.00 - FW1050.10 IBM Power HMC (7063-CR2) versions OP940.00 - OP940.70
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7163146

Affected Product	**PostgreSQL**
Severity	**High**
Affected Vulnerability	TOCTOU Race Condition Vulnerability (CVE-2024-7348)
Description	PostgreSQL has released security updates addressing a TOCTOU Race Condition Vulnerability that exists in their database management system. **CVE-2024-7348** - Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL Versions prior to 16.4, 15.8, 14.13, 13.16, and 12.20.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2024-7348/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information Disclosure, Remote Code Execution, Access Bypass. 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 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:5101 • https://access.redhat.com/errata/RHSA-2024:5102

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, memory corruption, use-after-free conditions. 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 Performance Computing 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242823-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242827-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242843-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242850-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242851-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242852-1/

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. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Denial of Service, Information Disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6949-1 • https://ubuntu.com/security/notices/USN-6950-1 • https://ubuntu.com/security/notices/USN-6951-1 • https://ubuntu.com/security/notices/USN-6952-1

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	SSH Terrapin Vulnerability (CVE-2023-48795)
Description	IBM has released security updates addressing the SSH Terrapin Vulnerability that affects IBM Storage products. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Storage products that use IBM Storage Virtualize versions 8.4, 8.5, 8.6 and 8.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7154643

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38474, CVE-2024-38475)
Description	F5 has released workarounds addressing multiple vulnerabilities that exist in BIG-IP systems. **CVE-2024-38474** - Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. **CVE-2024-38475** - Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions: • 17.x Branch - 17.1.0 - 17.1.1 • 16.x Branch - 16.1.0 - 16.1.5 • 15.x Branch - 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000140620

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Unchecked Return Value Vulnerability (CVE-2024-39558)
Description	Juniper has released security updates addressing an Unchecked Return Value Vulnerability that exists in Junos OS and Junos OS Evolved. **CVE-2024-39558** - An Unchecked Return Value vulnerability in the Routing Protocol Daemon (rpd) on Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows a logically adjacent, unauthenticated attacker sending a specific PIM packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS), when PIM is configured with Multicast-only Fast Reroute (MoFRR). Continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS: • All versions before 20.4R3-S10 • From 21.2 before 21.2R3-S7 • From 21.4 before 21.4R3-S6 • From 22.1 before 22.1R3-S5 • From 22.2 before 22.2R3-S3 • From 22.3 before 22.3R3 • From 22.4 before 22.4R2 Junos OS Evolved: • All versions before 20.4R3-S10 -EVO • All versions of 21.2-EVO • From 21.4-EVO before 21.4R3-S9-EVO • From 22.1-EVO before 22.1R3-S5 -EVO • From 22.2-EVO before 22.2R3-S3-EVO • From 22.3-EVO before 22.3R3-EVO • From 22.4-EVO before 22.4R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-specific-PIM-packet-causes-rpd-crash-when-PIM-is-configured-along-with-MoFRR-CVE-2024-39558?language=en_US

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.