Advisory Alert

Alert Number: AAA20241105 **Date:** November 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**Critical**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Qnap**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-50389)
Description	Qnap has released security updates addressing a critical vulnerability that exists in QuRouter. This vulnerability could be exploited by malicious users to compromise the affected system. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QuRouter 2.4.x versions before 2.4.5.032
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-45

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52752, CVE-2023-52846, CVE-2024-35817, CVE-2024-35861, CVE-2024-35862, CVE-2024-35863, CVE-2024-35864, CVE-2024-35867, CVE-2024-35905, CVE-2024-36899, CVE-2024-36964, CVE-2024-40909, CVE-2024-40954, CVE-2024-42133)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243884-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243882-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243880-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243881-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243885-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-34169, CVE-2022-48773, CVE-2022-48936, CVE-2023-52428, CVE-2023-52492, CVE-2024-24857, CVE-2024-26851, CVE-2024-26924, CVE-2024-26976, CVE-2024-27017, CVE-2024-27062, CVE-2024-35839, CVE-2024-35898, CVE-2024-35939, CVE-2024-38540, CVE-2024-38541, CVE-2024-38586, CVE-2024-38608, CVE-2024-39503, CVE-2024-4029, CVE-2024-40924, CVE-2024-40961, CVE-2024-40983, CVE-2024-40984, CVE-2024-41009, CVE-2024-41042, CVE-2024-41066, CVE-2024-41092, CVE-2024-41093, CVE-2024-41172, CVE-2024-42070, CVE-2024-42079, CVE-2024-42244, CVE-2024-42284, CVE-2024-42292, CVE-2024-42301, CVE-2024-43854, CVE-2024-43880, CVE-2024-43889, CVE-2024-43892, CVE-2024-44935, CVE-2024-44989, CVE-2024-44990, CVE-2024-45018, CVE-2024-46826, CVE-2024-47668, CVE-2024-8698, CVE-2024-8883)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 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 Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:8870 • https://access.redhat.com/errata/RHSA-2024:8856 • https://access.redhat.com/errata/RHSA-2024:8826 • https://access.redhat.com/errata/RHSA-2024:8824 • https://access.redhat.com/errata/RHSA-2024:8823

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.