# Advisory Alert

**Alert Number:** AAA20240709 **Date:** July 9, 2024

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Red Hat** | **High**, Medium | Multiple Vulnerabilities |
| **IBM** | **High**, Medium, Low | Multiple Vulnerabilities |
| **Node.js** | **High**, Medium, Low | Multiple Vulnerabilities |
| **Qnap** | Medium | Multiple Path Traversal Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-23307, CVE-2024-26828, CVE-2024-26923, CVE-2022-48651, CVE-2023-52340, CVE-2023-52502, CVE-2023-6546, CVE-2024-26585, CVE-2024-26610, CVE-2024-26622, CVE-2024-26766, CVE-2024-26852, CVE-2024-26930) |
| Description | SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Memory Corruption, Local Privilege Escalation, Denial of Service.<br><br>SUSE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | openSUSE Leap 15.5<br>SUSE Linux Enterprise High Performance Computing 15 SP5<br>SUSE Linux Enterprise Live Patching 15-SP5<br>SUSE Linux Enterprise Micro 5.5<br>SUSE Linux Enterprise Real Time 15 SP5<br>SUSE Linux Enterprise Server 15 SP5<br>SUSE Linux Enterprise Server for SAP Applications 15 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2024/suse-su-20242338-1/<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20242337-1/<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20242326-1/<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20242335-1/ |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High**, Medium |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-26555, CVE-2021-46909, CVE-2021-46972, CVE-2021-47069, CVE-2021-47073, CVE-2021-47236, CVE-2021-47310, CVE-2021-47311, CVE-2021-47353, CVE-2021-47356, CVE-2021-47456, CVE-2021-47495, CVE-2023-5090, CVE-2023-52464, CVE-2023-52560, CVE-2023-52615, CVE-2023-52626, CVE-2023-52667, CVE-2023-52700, CVE-2023-52703, CVE-2023-52781, CVE-2023-52813, CVE-2023-52835, CVE-2023-52877, CVE-2023-52878, CVE-2023-52881, CVE-2024-26583, CVE-2024-26584, CVE-2024-26585, CVE-2024-26656, CVE-2024-26675, CVE-2024-26735, CVE-2024-26759, CVE-2024-26801, CVE-2024-26804, CVE-2024-26826, CVE-2024-26859, CVE-2024-26906, CVE-2024-26907, CVE-2024-26974, CVE-2024-26982, CVE-2024-27397, CVE-2024-27410, CVE-2024-35789, CVE-2024-35835, CVE-2024-35838, CVE-2024-35845, CVE-2024-35852, CVE-2024-35853, CVE-2024-35854, CVE-2024-35855, CVE-2024-35888, CVE-2024-35890, CVE-2024-35958, CVE-2024-35959, CVE-2024-35960, CVE-2024-36004, CVE-2024-36007, CVE-2021-47400, CVE-2024-27393, CVE-2024-35870) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist their products. Exploitation of these vulnerabilities may lead to Information Disclosure, Security Bypass, Use-after-free conditions.<br><br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux for Real Time 8 x86_64<br>Red Hat Enterprise Linux for Real Time 9 x86_64<br>Red Hat Enterprise Linux for Real Time for NFV 8 x86_64<br>Red Hat Enterprise Linux for Real Time for NFV 9 x86_64<br>Red Hat Enterprise Linux for x86_64 9 x86_64<br>Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64<br>Red Hat Enterprise Linux Server - AUS 9.4 x86_64<br>Red Hat Enterprise Linux for IBM z Systems 9 s390x<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x<br>Red Hat Enterprise Linux for Power, little endian 9 ppc64le<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat Enterprise Linux for ARM 64 9 aarch64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64<br>Red Hat CodeReady Linux Builder for x86_64 9 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le<br>Red Hat CodeReady Linux Builder for ARM 64 9 aarch64<br>Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le<br>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64<br>Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64<br>Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x<br>Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64<br>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-2024:4352<br>• https://access.redhat.com/errata/RHSA-2024:4349 |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-35154, CVE-2021-43138, CVE-2023-35006, CVE-2023-33859, CVE-2023-33860, CVE-2023-35008, CVE-2024-34064, CVE-2024-4068, CVE-2024-34069, CVE-2024-3772, CVE-2024-1135, CVE-2024-29041, CVE-2024-34062, CVE-2024-35195, CVE-2024-4067, CVE-2024-29857, CVE-2024-29025, CVE-2024-25710, CVE-2024-26308, CVE-2024-30172, CVE-2023-33202, CVE-2024-28849) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Remote Code Execution, Arbitrary code Execution, Sensitive Information Disclosure, Cross-site Scripting, Denial of Service.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM WebSphere Application Server versions 9.0 and 8.5<br>IBM QRadar Deployment Intelligence App versions 1.0.0 - 3.0.13<br>IBM Security QRadar EDR versions 3.12<br>IBM Disconnected Log Collector versions 1.0 - 1.8.5<br>IBM Storage Ceph versions prior to 7.1, 6.1z1 - z6, 6.0, 5.3z1 - z6 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7159825<br>• https://www.ibm.com/support/pages/node/7159770<br>• https://www.ibm.com/support/pages/node/7159771<br>• https://www.ibm.com/support/pages/node/7159783<br>• https://www.ibm.com/support/pages/node/7159781<br>• https://www.ibm.com/support/pages/node/7159823 |

| | |
|---|---|
| Affected Product | **Node.js** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-36138, CVE-2024-22020, CVE-2024-36137, CVE-2024-22018, CVE-2024-37372) |
| Description | Node.js has released security updates addressing multiple vulnerabilities that exist in Node.js environments. Exploitation of these vulnerabilities may lead to Arbitrary Command Injection, Permission Bypass.<br>Node.js advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Node.js releases 22.x, 20.x, 18.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://nodejs.org/en/blog/vulnerability/july-2024-security-releases#bypass-incomplete-fix-of-cve-2024-27980-cve-2024-36138---high |

| | |
|---|---|
| Affected Product | **Qnap** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Path Traversal Vulnerabilities (CVE-2023-41290, CVE-2023-41291) |
| Description | Qnap has released security updates addressing multiple Path Traversal vulnerabilities that exist in QuFirewall. If exploited, these vulnerabilities could allow remote attackers to read sensitive data.<br>Qnap advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | QuFirewall versions prior to 2.4.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.qnap.com/en/security-advisory/qsa-24-17 |

**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.**