# Advisory Alert

**Alert Number:** AAA20240318 **Date:** March 18, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **QNAP** | **Critical** | Multiple Vulnerabilities |
| **Suse** | **High** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **QNAP** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-21899, CVE-2024-21900, CVE-2024-21901) |
| Description | QNAP has issued security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could be exploited by malicious users to compromise the affected system.<br>**CVE-2024-21899** - The improper authentication vulnerability could allow users to compromise the security of the system via a network.<br>**CVE-2024-21900** - The injection vulnerability could allow authenticated users to execute commands via a network.<br>**CVE-2024-21901** - SQL injection vulnerability could allow authenticated administrators to inject malicious code via a network.<br>QNAP recommends to apply security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | QTS 5.x<br>QTS 4.5.x<br>QuTS hero h5.x<br>QuTS hero h4.5.x<br>QuTScloud c5.x<br>myQNAPcloud 1.0.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.qnap.com/en/security-advisory/qsa-24-09 |

| | |
|---|---|
| Affected Product | **Suse** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2019-25162, CVE-2021-46923, CVE-2021-46924, CVE-2021-46932, CVE-2023-28746, CVE-2023-5197, CVE-2023-52340, CVE-2023-52429, CVE-2023-52439, CVE-2023-52443, CVE-2023-52445, CVE-2023-52447, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52452, CVE-2023-52456, CVE-2023-52457, CVE-2023-52463, CVE-2023-52464, CVE-2023-52475, CVE-2023-52478, CVE-2024-0607, CVE-2024-1151, CVE-2024-23849, CVE-2024-23850, CVE-2024-23851, CVE-2024-25744, CVE-2024-26585, CVE-2024-26586, CVE-2024-26589, CVE-2024-26591, CVE-2024-26593, CVE-2024-26595, CVE-2024-26598, CVE-2024-26602, CVE-2024-26603, CVE-2024-26622) |
| Description | Suse has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Out-of-Bounds Memory Access, Use-After-Free ,NULL Pointer Dereference.<br>Suse recommends to apply security fixes at your earliest to protect your 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<br>SUSE Real Time Module 15-SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2024/suse-su-20240910-1/ |

### 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.**