# Advisory Alert

**Alert Number:** AAA20241125 **Date:** November 25, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **QNAP** | **High**, **Medium** | Multiple Vulnerabilities |
| **F5** | **Medium** | NULL Pointer Dereference Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-7238, CVE-2020-28052, CVE-2021-3859, CVE-2021-4104, CVE-2022-23221, CVE-2022-23305, CVE-2022-23307, CVE-2022-34169, CVE-2022-41853, CVE-2022-46364, CVE-2023-3171, CVE-2023-5685, CVE-2023-26464, CVE-2023-39410, CVE-2024-28752, CVE-2024-47561) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Denial Of Service, Heap Exhaustion Via Deserialization.<br><br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64<br>JBoss Enterprise Application Platform 7.3 EUS 7.3 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2024:10208<br>• https://access.redhat.com/errata/RHSA-2024:10207 |

| | |
|---|---|
| Affected Product | **QNAP** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-14145, CVE-2021-41617, CVE-2023-38408, CVE-2024-37041, CVE-2024-37042, CVE-2024-37043, CVE-2024-37044, CVE-2024-37045, CVE-2024-37046, CVE-2024-37047, CVE-2024-37048, CVE-2024-37049, CVE-2024-37050, CVE-2024-38647, CVE-2024-48860, CVE-2024-48861, CVE-2024-48862, CVE-2024-50396, CVE-2024-50397, CVE-2024-50398, CVE-2024-50399, CVE-2024-50400) |
| Description | QNAP has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause NULL Pointer Dereference, Denial-Of-Service, Path Traversal, Execute Arbitrary Commands<br><br>QNAP advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | QTS 5.1.x versions before 5.1.8.2823 build 20240712<br>QuTS hero h5.1.x versions before h5.1.8.2823 build 20240712<br>QNAP AI Core 3.4.x versions before Core 3.4.1<br>QuLog Center 1.7.x versions before 1.7.0.831 (2024/10/15)<br>QuLog Center 1.8.x versions before 1.8.0.888 (2024/10/15)<br>QTS 5.2.x versions before 5.2.1.2930 build 20241025<br>QuTS hero h5.2.x versions before h5.2.1.2929 build 20241025<br>QuRouter 2.4.x versions before 2.4.3.106 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.qnap.com/en/security-advisory/qsa-24-37<br>• https://www.qnap.com/en/security-advisory/qsa-24-40<br>• https://www.qnap.com/en/security-advisory/qsa-24-46<br>• https://www.qnap.com/en/security-advisory/qsa-24-43<br>• https://www.qnap.com/en/security-advisory/qsa-24-44 |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **Medium** |
| Affected Vulnerability | NULL Pointer Dereference Vulnerability (CVE-2023-1667) |
| Description | F5 has issued security updates addressing a NULL Pointer Dereference Vulnerability that exists in their products.<br><br>**CVE-2023-1667 -** A NULL pointer dereference was found In libssh during re-keying with algorithm guessing. This issue may allow an authenticated client to cause a denial of service<br><br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | BIG-IP (AFM) 17.x 17.1.0 - 17.1.1<br>BIG-IP (AFM) 16.x 16.1.0 - 16.1.4<br>BIG-IP (AFM) 15.x 15.1.0 - 15.1.10 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://my.f5.com/manage/s/article/K000148495 |

**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.**