



Advisory Alert

Alert Number: AAA20231106

Date: November 6, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	Critical	OS Command Injection Vulnerabilities
Suse	High	Multiple Vulnerabilities
Qnap	Medium	Server-Side Request Forgery (SSRF) Vulnerability

Description

Affected Product	Qnap
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23369, CVE-2023-23368)
Description	<p>Qnap has released a security update addressing OS command injection vulnerabilities.</p> <p>CVE-2023-23369 - An OS command injection vulnerability has been reported to affect several QNAP operating system and application versions. If exploited, the vulnerability could allow remote attackers to execute commands via a network.</p> <p>CVE-2023-23368 - An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow remote attackers to execute commands via a network.</p> <p>Qnap strongly recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	QuTScld c5.0.x QuTS hero h5.0.x QuTS hero h4.5.x QTS 5.1.x QTS 5.0.x QTS 4.5.x QTS 4.3.6 QTS 4.3.4 QTS 4.3.3 QTS 4.2.x Multimedia Console 2.1.x Multimedia Console 1.4.x Media Streaming add-on 500.1.x Media Streaming add-on 500.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/go/security-advisory/qa-23-35 https://www.qnap.com/go/security-advisory/qa-23-31

Affected Product	Suse
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2163, CVE-2023-3111, CVE-2023-34324, CVE-2023-3777, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-42754, CVE-2023-31085, CVE-2023-45862)
Description	<p>Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Arbitrary read/write, Privilege escalation, Out of bounds read.</p> <p>Suse recommends to apply the necessary security updates at earliest to avoid issues</p>
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234358-1 https://www.suse.com/support/update/announcement/2023/suse-su-20234359-1

Affected Product	Qnap
Severity	Medium
Affected Vulnerability	Server-Side Request Forgery (SSRF) Vulnerability (CVE-2023-39301)
Description	<p>Qnap has released a security update addressing a multiple server-side request forgery (SSRF) vulnerability.</p> <p>CVE-2023-39301 - The vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to read application data via a network.</p> <p>Qnap highly recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	QTS 5.1.x QTS 5.0.x QuTS hero h5.1.x QuTS hero h5.0.x QuTScld c5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/go/security-advisory/qa-23-51

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.