Advisory Alert

Alert Number: **AAA20230731** **Date:** **July 31, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**High**	Path Traversal Vulnerability
Qnap	**High**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2023-35081)
Description	Ivanti has released a security update addressing a Path Traversal Vulnerability in Ivanti Endpoint Manager Mobile. If exploited, an attacker with administrator privileges could be able to write arbitrary files with the operating system privileges of the Ivanti Endpoint Manager Mobile web application server Ivanti recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) all supported versions –releases 11.10, 11.9 and 11.8. and Older versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

Affected Product	**Qnap**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27600, CVE-2022-27595)
Description	Qnap has released security updates addressing Multiple Vulnerabilities. If exploited, these Vulnerabilities could lead to arbitrary code execution and denial-of-service. **CVE-2022-27600 -** Resource exhaustion vulnerability exists because the application does not properly control consumption of internal resources. A remote user can trigger resource exhaustion and perform a denial of service attack. **CVE-2022-27595 -** An improper input validation vulnerability exists due to insecure library loading. A local user can load an insecure library and execute arbitrary code on the target system. Qnap recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	QNAP QTS: before 5.0.1.2277 build 20230112 QNAP QTS: before 4.5.4.2280 build 20230112 QuTS hero: before h5.0.1.2277 build 20230112 QuTS hero: before h4.5.4.2374 build 20230417 QuTScloud: before c5.0.1.2374 build 20230419 QVP (QVR Pro appliances): before 2.3.1.0476 QVPN Device Client for Windows: before 2.0.0.1316
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-04 https://www.qnap.com/en/security-advisory/qsa-23-09

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.