Advisory Alert

Alert Number: **AAA20231016** **Date:** **October 16, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**High**, **Medium**	Multiple Vulnerabilities
Juniper	**High**, **Medium**	Multiple Vulnerabilities
NodeJS	**High**, **Medium** , **Low**	Multiple Vulnerabilities
Fortinet	**High**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Qnap**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32976, CVE-2023-32974, CVE-2023-32973, CVE-2023-32970, CVE-2023-34975, CVE-2023-34976, CVE-2023-34977)
Description	Qnap has released security updates addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to SQL injection, Cross-site scripting, denial-of-service, Sensitive information disclosure Qnap recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Container Station 2.6.x Before version 2.6.7.44 QTS 5.1.x Before version 5.1.0.2444 build 20230629 QuTS hero h5.1.x Before version h5.1.0.2424 build 20230609 QuTScloud c5.x Before version c5.1.0.2498 QTS 5.0.x Before version 5.0.1.2425 build 20230609 QTS 4.5.x Before version 4.5.4.2467 build 20230718 QuTS hero h5.0.x Before version h5.0.1.2515 build 20230907
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-44 https://www.qnap.com/en/security-advisory/qsa-23-42 https://www.qnap.com/en/security-advisory/qsa-23-41 https://www.qnap.com/en/security-advisory/qsa-23-52

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-36839, CVE-2023-44204, CVE-2023-44182, CVE-2023-44203, CVE-2023-44202, CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554, CVE-2023-26555, CVE-2023-44197, CVE-2023-44195, CVE-2023-44187, CVE-2023-44201, CVE-2023-44199, CVE-2023-44181, CVE-2023-44188, CVE-2023-22392, CVE-2022-2097, CVE-2022-2274, CVE-2023-44192, CVE-2023-44175, CVE-2023-44176, CVE-2023-44177, CVE-2023-44178, CVE-2023-36841, CVE-2023-36843, CVE-2023-44193, CVE-2023-44183, CVE-2023-44185, CVE-2023-44190, CVE-2023-44189)
Description	Juniper has released security update addressing Multiple Vulnerabilities in Juniper Networks Junos OS and Junos OS Evolved. Successful exploitation of these vulnerabilities could lead to Denial of Service, sensitive information disclosure, Code Injections and Deletion Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Junos OS and Junos OS Evolved Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&numberOfResults=50=50&f:ctype=[Security%20Advisories]&f:level1=[Security%20Advisories]

Affected Product	**Node.js**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45143, CVE-2023-44487, CVE-2023-39331, CVE-2023-39332, CVE-2023-38552, CVE-2023-39333)
Description	Node.js has released security updates addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to Path traversal, denial-of-service, Code injection Node.js recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Node.js Version Before v20.8.1 (Current) Node.js Version Before v18.18.2 (LTS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/october-2023-security-releases

Affected Product	**Fortinet**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41680, CVE-2023-41836, CVE-2023-41682, CVE-2023-41843)
Description	Fortinet has released security updates addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to Reflected Cross Site Scripting and Arbitrary file delete Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiSandbox 2.4 all versions FortiSandbox 2.5 all versions FortiSandbox 3.2 all versions FortiSandbox version 4.0.0 through 4.0.3 FortiSandbox version 4.2.0 through 4.2.5 FortiSandbox version 4.4.0 through 4.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-273 https://www.fortiguard.com/psirt/FG-IR-23-280 https://www.fortiguard.com/psirt/FG-IR-23-215 https://www.fortiguard.com/psirt/FG-IR-23-311

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.