



Advisory Alert

Alert Number: AAA20240311

Date: March 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	Critical	Multiple Vulnerabilities
QNAP	Critical	Multiple Vulnerabilities
Juniper	High	Improper Handling of Exceptional Conditions vulnerability
Ivanti	High, Medium	Multiple Vulnerabilities
QNAP	Medium	Multiple Vulnerabilities

Description

Affected Product	Ivanti
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41727, CVE-2023-46216, CVE-2023-46217, CVE-2023-46220, CVE-2023-46221, CVE-2023-46222, CVE-2023-46223, CVE-2023-46224, CVE-2023-46225, CVE-2023-46257, CVE-2023-46258, CVE-2023-46259, CVE-2023-46261)
Description	Ivanti has issued security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could be exploited by corrupting memory which could result to a Denial of Service or code execution. Ivanti advises to apply security fixes at earliest to avoid problems.
Affected Products	Ivanti Avalanche versions prior to 6.4.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-6-4-2-Security-Hardening-and-CVEs-addressed?language=en_US

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. CVE-2024-21899 - The improper authentication vulnerability could allow users to compromise the security of the system via a network. CVE-2024-21900 - The injection vulnerability could allow authenticated users to execute commands via a network. CVE-2024-21901 - SQL injection vulnerability could allow authenticated administrators to inject malicious code via a network. QNAP advises to apply security fixes at earliest to avoid problems.
Affected Products	QTS 5.1.x QTS 4.5.x QuTS hero h5.1.x QuTS hero h4.5.x QuTScldoud c5.x myQNAPcloud 1.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qa-24-09

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Affected Product	Juniper
Severity	High
Affected Vulnerability	Improper Handling of Exceptional Conditions vulnerability (CVE-2023-44186)
Description	<p>Juniper has released security updates addressing multiple vulnerabilities that exist in Junos OS and Junos OS Evolved. These vulnerabilities could be exploited by malicious users to cause Denial of Service attacks.</p> <p>CVE-2023-44186 - An Improper Handling of Exceptional Conditions vulnerability in AS PATH processing of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a BGP update message with an AS PATH containing a large number of 4-byte ASes, leading to a Denial of Service (DoS).</p> <p>Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	<p>Junos OS All versions prior to 20.4R3-S8; Junos OS 21.1 versions 21.1R1 and later; Junos OS 21.2 versions prior to 21.2R3-S6; Junos OS 21.3 versions prior to 21.3R3-S5; Junos OS 21.4 versions prior to 21.4R3-S5; Junos OS 22.1 versions prior to 22.1R3-S4; Junos OS 22.2 versions prior to 22.2R3-S2; Junos OS 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; Junos OS 22.4 versions prior to 22.4R2-S1, 22.4R3. Junos OS Evolved All versions prior to 20.4R3-S8-EVO; Junos OS Evolved 21.1 versions 21.1R1-EVO and later; Junos OS Evolved 21.2 versions prior to 21.2R3-S6-EVO; Junos OS Evolved 21.3 versions prior to 21.3R3-S5-EVO; Junos OS Evolved 21.4 versions prior to 21.4R3-S5-EVO; Junos OS Evolved 22.1 versions prior to 22.1R3-S4-EVO; Junos OS Evolved 22.2 versions prior to 22.2R3-S2-EVO; Junos OS Evolved 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; Junos OS Evolved 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO.</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-attempting-to-send-a-very-long-AS-PATH-to-a-non-4-byte-AS-capable-BGP-neighbor-CVE-2023-44186?language=en_US

Affected Product	Ivanti
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46260, CVE-2023-46262, CVE-2023-46266, CVE-2023-46263, CVE-2021-22962, CVE-2023-46264, CVE-2023-46265, CVE-2023-46803, CVE-2023-46804, CVE-2023-22809, CVE-2023-28324)
Description	<p>Ivanti has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to privilege escalation, Denial of Service, Remote Code Execution, Server-Side Request Forgery, Session Takeover and Authentication Bypass vulnerabilities.</p> <p>Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.</p>
Affected Products	<p>Ivanti Avalanche versions prior to 6.4.2 EPM 2022 SU2 and prior versions EPMM, Sentry and Connector</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<p>https://forums.ivanti.com/s/article/Avalanche-6-4-2-Security-Hardening-and-CVEs-addressed?language=en_US https://forums.ivanti.com/s/article/Impact-of-CVE-2023-22809-on-EPMM-Sentry-and-Connector?language=en_US https://forums.ivanti.com/s/article/SA-2023-06-06-CVE-2023-28324?language=en_US https://forums.ivanti.com/s/article/ZDI-CAN-17812-Ivanti-Avalanche-FileStoreConfig-Arbitrary-File-Upload-Remote-Code-Execution-Vulnerability?language=en_US https://forums.ivanti.com/s/article/ZDI-CAN-17769-Ivanti-Avalanche-getLogFile-Directory-Traversal-Information-Disclosure?language=en_US https://forums.ivanti.com/s/article/ZDI-CAN-17750-Ivanti-Avalanche-EnterpriseServer-GetSettings-Exposed-Dangerous-Method-Authentication-Bypass-Vulnerability?language=en_US</p>

Affected Product	QNAP
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32969, CVE-2023-34975, CVE-2023-34980)
Description	<p>QNAP has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these could allow a remote attacker to inject malicious code via a network and command execution vulnerabilities.</p> <p>CVE-2023-32969 - A cross-site scripting (XSS) vulnerability has been reported to affect Network & Virtual Switch. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network.</p> <p>CVE-2023-34975 - An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network.</p> <p>CVE-2023-34980 - An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network.</p> <p>It is recommended by QNAP to apply necessary security fixes at earliest to avoid issues.</p>
Affected Products	QTS 5.1.x, 4.5.x QuTS hero h5.1.x, h4.5.x QuTScld c5.x, c5.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qa-24-11 https://www.qnap.com/en/security-advisory/qa-24-12

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.