Advisory Alert

Alert Number: AAA20240827 **Date:** August 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	Improper Access Control Vulnerability
Qnap	**Critical**	Multiple vulnerabilities
Dell	**High**	OpenSSH's Server Security Regression
Qnap	**High**	Multiple Vulnerabilities

Description

Affected Product	**SonicWall**
Severity	**Critical** - Initial release date **23rd August 2024 (AAA20240823)**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2024-40766)
Description	SonicWall has released security updates addressing an Improper Access Control Vulnerability that exists in SonicOS management access. **CVE-2024-40766** - An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall Firewall Gen 5 devices running SonicOS 5.9.2.14-12o and older versions. SonicWall Firewall Gen 6 devices running SonicOS 6.5.4.14-109n and older versions. SonicWall Firewall Gen 7 devices running SonicOS 7.0.1-5035 and older versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

Affected Product	**Qnap**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21899, CVE-2024-21900, CVE-2024-21901, CVE-2024-27124, CVE-2024-32764, CVE-2024-32766)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Arbitrary Command Execution, Privilege Escalation, Malicious Code Injection. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.x QTS 4.5.x QuTS hero h5.x QuTS hero h4.5.x QuTScloud c5.x myQNAPcloud 1.0.x myQNAPcloud Link 2.4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-09

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	OpenSSH's Server Security Regression (CVE-2024-6387)
Description	Dell has released security updates addressing a Security Regression that exists in OpenSSH's server which affects Dell Hybrid Client. **CVE-2024-6387** - A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Secure Shell (SSH) Addon Package (version 8.9p1-3-05_22.04) on Dell Hybrid Client versions 2310 and 2403 of • Latitude 3440 • Latitude 3450 • Latitude 5440 • Latitude 5450 • OptiPlex 3000 Thin Client • OptiPlex 7410 All-In-One • OptiPlex 7420 All-In-One • Precision 3280 • Precision 3260
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227596/dsa-2024-356

Affected Product	**Qnap**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51364, CVE-2023-51365, CVE-2024-32765)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-51364** and **CVE-2023-51365** - If exploited, the path traversal vulnerabilities could allow remote attackers who have gained user access to traverse the file system and read sensitive data. **CVE-2024-32765** - If exploited, the vulnerability could allow attackers to gain access to the system and execute certain functions. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.1.x QTS 4.5.x QuTS hero h5.1.x QuTS hero h4.5.x QuTScloud c5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-14

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.