TLP: WHITE

Advisory Alert

Alert Number: AAA20230131 **Date:** January 31, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**Critical**	Arbitrary SQL queries Execution Vulnerability
RedHat	**High**	Multiple Vulnerabilities

Description

Affected Product	**Qnap**
Severity	**Critical**
Affected Vulnerability	Arbitrary SQL queries Execution Vulnerability (CVE-2022-27596)
Description	Qnap has released a Security Update addressing an Arbitrary SQL queries execution Vulnerability that exist in their products. A remote attacker can send a specially crafted request to the affected device and execute arbitrary SQL commands within the application database. Successful exploitation of this vulnerability may allow a remote attacker to inject and execute arbitrary code on the system Qnap highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	QTS 5.0.1 QuTS hero h5.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-01

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2414, CVE-2022-4883, CVE-2022-4283, CVE-2022-46340, CVE-2022-46341, CVE-2022-46342, CVE-2022-46343, CVE-2022-46344)
Description	RedHat has released Security Updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause privilege escalation, remote code execution, malicious user to execute other programs, arbitrary file writes. RedHat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8799 https://access.redhat.com/errata/RHSA-2023:0377 https://access.redhat.com/errata/RHSA-2023:0046

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.