Advisory Alert

Alert Number: AAA20241030 **Date:** October 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**Critical**	OS Command Injection Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Qnap**
Severity	**Critical**
Affected Vulnerability	OS command injection Vulnerability (CVE-2024-50388)
Description	Qnap has released security updates addressing an OS Command Injection Vulnerability that exists in their products. **CVE-2024-50388** - An OS command injection vulnerability has been reported to affect HBS 3 Hybrid Backup Sync. If exploited, the vulnerability could allow remote attackers to execute arbitrary commands. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HBS 3 Hybrid Backup Sync 25.1.x versions before 25.1.1.673
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-41

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-7207, CVE-2024-23651, CVE-2024-23653, CVE-2024-23652, CVE-2024-0553, CVE-2023-5981, CVE-2024-26458, CVE-2024-26461, CVE-2024-32487, CVE-2020-1730, CVE-2023-6918, CVE-2023-1667, CVE-2023-48795, CVE-2023-6004, CVE-2020-16135, CVE-2019-14889, CVE-2023-2283, CVE-2021-3634, CVE-2024-25062, CVE-2023-1829, CVE-2023-23559, CVE-2024-28182, CVE-2023-5388, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2024-21094, CVE-2024-21012, CVE-2024-21068, CVE-2024-21011, CVE-2024-21085, CVE-2023-51385, CVE-2024-2511, CVE-2024-22365, CVE-2018-6913, CVE-2017-6512, CVE-2018-6798, CVE-2023-31484, CVE-2024-0985, CVE-2023-52425, CVE-2024-0450, CVE-2024-21626, CVE-2023-42465, CVE-2024-28085, CVE-2023-4733, CVE-2023-4738, CVE-2023-4781, CVE-2023-5535, CVE-2023-4750, CVE-2023-4752, CVE-2024-22667, CVE-2023-5441, CVE-2023-5344, CVE-2023-46246, CVE-2023-48231, CVE-2023-48232, CVE-2023-48706, CVE-2023-4734, CVE-2023-4735, CVE-2023-48233, CVE-2023-48234, CVE-2023-48236, CVE-2023-48237, CVE-2023-48235, CVE-2023-46839)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect Dell PowerStoreX OS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerStoreX OS versions prior to 3.2.1.4-2386214 running on • Dell PowerStore 1000X • Dell PowerStore 3000X • Dell PowerStore 5000X • Dell PowerStore 7000X • Dell PowerStore 9000X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000242275/dsa-2024-432-dell-powerstore-x-security-update-for-multiple-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47291, CVE-2021-47598, CVE-2024-41059, CVE-2023-52752, CVE-2024-35862, CVE-2024-35863, CVE-2024-35864, CVE-2024-35867, CVE-2024-26923, CVE-2024-35861, CVE-2024-35950, CVE-2024-36964, CVE-2021-47600)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3, 15-SP4, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP6 SUSE Linux Enterprise Server 15 SP2, 15 SP3, 15 SP4, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP3, 15 SP4, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243779-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243777-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243775-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243774-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243768-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47383, CVE-2024-2201, CVE-2024-26640, CVE-2024-26826, CVE-2024-26923, CVE-2024-26935, CVE-2024-26961, CVE-2024-36244, CVE-2024-39472, CVE-2024-39504, CVE-2024-40904, CVE-2024-40931, CVE-2024-40960, CVE-2024-40972, CVE-2024-40977, CVE-2024-40995, CVE-2024-40998, CVE-2024-41005, CVE-2024-41013, CVE-2024-41014, CVE-2024-43854, CVE-2024-45018, CVE-2022-48773, CVE-2021-47384, CVE-2023-1252, CVE-2023-52489, CVE-2024-26671, CVE-2024-26686, CVE-2024-36889, CVE-2024-41049, CVE-2024-41055, CVE-2024-42152, CVE-2024-41064)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x , 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64, AUS 9.2 x86_64, AUS 9.4 x86_64, TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le -IP (all modules) 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:8617 • https://access.redhat.com/errata/RHSA-2024:8616 • https://access.redhat.com/errata/RHSA-2024:8614 • https://access.redhat.com/errata/RHSA-2024:8613

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.