Advisory Alert

Alert Number: **AAA20240802** **Date:** **August 2, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Race Condition Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116, CVE-2022-21797, CVE-2023-46228, CVE-2024-1597, CVE-2018-6594, CVE-2020-14387)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell products. 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 3.2.1.3-2334099 in • PowerStore 1000X • PowerStore 3000X • PowerStore 5000X • PowerStore 7000X • PowerStore 9000X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227490/dsa-2024-336-dell-powerstore-x-security-update-for-multiple-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell products. 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	Dell SmartFabric OS10 10.5.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227497/dsa-2024-333-security-update-for-dell-os10-third-party-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-20843, CVE-2019-15903, CVE-2021-46143, CVE-2022-22825, CVE-2022-23990, CVE-2020-24977, CVE-2021-3517, CVE-2021-3518, CVE-2021-3537, CVE-2021-3541, CVE-2022-40304, CVE-2022-40303, CVE-2023-28484,CVE-2023-29469, CVE-2024-5462, CVE-2024-5461)
Description	HPE has released security updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service (DoS), Disclosure of Sensitive Information, Unauthorized Data Modification, Unauthorized Read Access to Data, Buffer Overflow, Stack Overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE SN8700B 4-slot SAN Director Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE SN8700B 8-slot SAN Director Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE SN8600B 4-slot SAN Director Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE SN8600B 8-slot SAN Director Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN2600B SAN Extension Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN3600B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN4700B SAN Extension Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6000B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6500B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6600B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6650B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6700B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1 HPE B-series SN6750B Fibre Channel Switch - Prior to v9.1.1d2, v9.2.0b1, v9.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04679en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Race Condition Vulnerability (CVE-2023-6546)
Description	Red Hat has released security updates addressing a Race Condition Vulnerability that exists in their products. This issue occurs when two threads execute the GSMIOC_SETCONF ioctl on the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struct gsm_dlci while restarting the gsm mux. This could allow a local unprivileged user to escalate their privileges on the system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:4970

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.