TLP: WHITE

Advisory Alert

Alert Number: AAA20240919 **Date:** September 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
Drupal	**High**	Access Bypass Vulnerability
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Use After Free Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
SolarWinds	**Medium**	Hard-Coded Credential Authentication Bypass Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical** - Initial release date **13th September 2024 (AAA20240913)**
Affected Vulnerability	Security Update (CVE-2023-37920)
Description	NetApp has released a security update addressing multiple vulnerabilities that exist in Certifi which affect NetApp products. Multiple Certifi versions are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Certifi versions 2015.04.28 prior to 2023.07.22 that are used in, • ONTAP Select Deploy administration utility • Management Services for Element Software and NetApp HCI • ONTAP Mediator
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240912-0002/

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released security updates addressing an Access Bypass Vulnerability that exists in Smart IP Ban module. The module doesn't sufficiently protect access to certain paths provided by the module allowing a malicious user to view and modify the settings. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Smart IP Ban module for Drupal versions prior to 7.x-1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-041

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42772, CVE-2024-21829, CVE-2024-21871, CVE-2023-43753, CVE-2024-21781)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Disclosure of Information and Escalation of Privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE StoreEasy 1660 Storage - Prior to v2.20_08-07-2024 (U46 ROM Family) or prior to v3.30_07-31-2024 (U30 ROM Family) HPE StoreEasy 1860 Storage - Prior to v2.20_08-07-2024 (U46 ROM Family) or prior to v3.30_07-31-2024 (U30 ROM Family) HPE StoreEasy 1670 Expanded Storage - Prior to v2.20_08-07-2024 (U50 ROM Family) HPE StoreEasy 1860 Expanded Storage - Prior to v2.20_08-07-2024 (U50 ROM Family) HPE StoreEasy 1870 Expanded Storage - Prior to v2.20_08-07-2024 (U50 ROM Family) HPE StoreEasy 1460 Storage - Prior to v3.30_07-31-2024 (U32 ROM Family) HPE StoreEasy 1560 Storage - Prior to v3.30_07-31-2024 (U32 or U30 ROM Families) HPE StoreEasy 1660 Expanded Storage - Prior to v3.30_07-31-2024 (U39 ROM Family) HPE StoreEasy 1660 Performance Storage - Prior to v3.30_07-31-2024 (U30 ROM Family) HPE StoreEasy 1860 Performance Storage - Prior to v3.30_07-31-2024 (U32 ROM Family) HPE Storage File Controller - Prior to v3.30_07-31-2024 (U32 ROM Family) HPE Storage Performance File Controller - Prior to v3.30_07-31-2024 (U32 ROM Family) HPE StoreEasy 1450 Storage - Prior to v3.40_08-29-2024 (P89 ROM Family) HPE StoreEasy 1550 Storage - Prior to v3.40_08-29-2024 (P99 ROM Family) HPE StoreEasy 1650 Storage - Prior to v3.40_08-29-2024 (P89 ROM Family) HPE StoreEasy 1850 Storage - Prior to v3.40_08-29-2024 (P89 ROM Family) HPE StoreEasy 1650 Expanded Storage - Prior to v3.40_08-29-2024 (U19 ROM Family) HPE StoreEasy 3850 Gateway Storage - Prior to v3.30_07-31-2024 (U14 ROM Family) HPE 3PAR StoreServ File Controller v3 System - Prior to v3.30_07-31-2024 (U14 ROM Family)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04704en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Use After Free Vulnerability (CVE-2022-48791)
Description	SUSE has released security updates addressing a Use After Free Vulnerability that exists in their products. **CVE-2022-48791** - Currently a use-after-free may occur if a TMF sas_task is aborted before we handle the IO completion in mpi_ssp_completion(). The abort occurs due to timeout. When the timeout occurs, the SAS_TASK_STATE_ABORTED flag is set and the sas_task is freed in pm8001_exec_internal_tmf_task(). SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243304-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21138, CVE-2024-21131, CVE-2024-27267)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in Db2 Query Management Facility. These vulnerabilities could be exploited by malicious users to cause Denial of Service, confidentiality, availability and integrity impacts. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DB2 Query Management Facility for z/OS versions 12.2, 13.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7168925

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7022-1 • https://ubuntu.com/security/notices/USN-7021-1 • https://ubuntu.com/security/notices/USN-7020-1 • https://ubuntu.com/security/notices/USN-7019-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47352, CVE-2021-47492, CVE-2022-48687, CVE-2024-26704, CVE-2024-26772, CVE-2024-26773, CVE-2024-27019, CVE-2024-27020, CVE-2024-35898, CVE-2024-41009)
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 Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - 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 for x86_64 - Update Services for SAP Solutions 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:6753

Affected Product	**SolarWinds**
Severity	**Medium**
Affected Vulnerability	Hard-Coded Credential Authentication Bypass Vulnerability (CVE-2024-28990)
Description	SolarWinds has released security updates addressing a Hard-Coded Credential Authentication Bypass Vulnerability that exists in SolarWinds Access Rights Manager. If exploited, this vulnerability would allow access to the RabbitMQ management console. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds ARM 2024.3 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28990

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.