Advisory Alert

Alert Number: AAA20240813 **Date:** August 13, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**Medium**	Heap Buffer Overflow Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1017, CVE-2023-1018, CVE-2024-22254, CVE-2024-22274, CVE-2024-22275, CVE-2024-37079, CVE-2024-37080, CVE-2024-37081, CVE-2024-37087, CVE-2023-48795, CVE-2023-0461, CVE-2023-31083, CVE-2023-39197, CVE-2023-39198, CVE-2023-45863, CVE-2023-45871, CVE-2023-5717, CVE-2023-46589, CVE-2024-23672, CVE-2024-24549, CVE-2023-50868, CVE-2023-4408)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerProtect DP Series Appliance (Integrated Data Protection Appliance) Versions 2.7.6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227707/dsa-2024-157-security-update-for-dell-powerprotect-dp-series-appliance-idpa-infrastructure-for-third-party-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26923, CVE-2024-27398, CVE-2024-35950)
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 systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20242874-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47459, CVE-2022-36402, CVE-2022-38457, CVE-2022-40133, CVE-2022-48743, CVE-2023-5633, CVE-2023-33951, CVE-2023-33952, CVE-2023-52434, CVE-2023-52439, CVE-2023-52450, CVE-2023-52518, CVE-2023-52578, CVE-2023-52707, CVE-2023-52811, CVE-2024-1151, CVE-2024-26581, CVE-2024-26668, CVE-2024-26698, CVE-2024-26704, CVE-2024-26739, CVE-2024-26773, CVE-2024-26808, CVE-2024-26810, CVE-2024-26880, CVE-2024-26908, CVE-2024-26923, CVE-2024-26925, CVE-2024-26929, CVE-2024-26931, CVE-2024-26982, CVE-2024-27016, CVE-2024-27019, CVE-2024-27020, CVE-2024-27065, CVE-2024-27417, CVE-2024-35791, CVE-2024-35897, CVE-2024-35899, CVE-2024-35950, CVE-2024-36025, CVE-2024-36489, CVE-2024-36904, CVE-2024-36924, CVE-2024-36952, CVE-2024-36978, CVE-2024-38596)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to use after free conditions, denial of service, use-after-free remote code execution, Resource Leak. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:5261 • https://access.redhat.com/errata/RHSA-2024:5259 • https://access.redhat.com/errata/RHSA-2024:5257 • https://access.redhat.com/errata/RHSA-2024:5256 • https://access.redhat.com/errata/RHSA-2024:5255

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 cause Arbitrary Code Execution, Denial of Service, Information Disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6955-1

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Heap Buffer Overflow Vulnerability (CVE-2020-15999)
Description	NetApp has released security updates addressing a Heap Buffer Overflow Vulnerability that exists in third party products that affect NetApp ONTAP products. Certain Freetype versions are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP Select Deploy administration utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240812-0001/

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.