Advisory Alert

Alert Number: AAA20240912 **Date:** September 12, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Denial of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Palo Alto	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities
Drupal	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Data Protection Central DPC-OS update versions prior to 1.1.19-1 PowerProtect DP Series (IDPA) DPC-OS update versions prior to 1.1.19-1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228490/dsa-2024-395-security-update-for-dell-data-protection-central-for-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2012-0876, CVE-2021-3520, CVE-2022-43680, CVE-2023-52425, CVE-2023-52426, CVE-2024-28757)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in Virtual Tape Repository. These vulnerabilities could be exploited by malicious users to compromise the affected system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Virtual Tape Repository T0964V01, T0964V01^AAA to AAJ
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbns04698en_us&docLocale=en_US

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-52340)
Description	NetApp has released security updates addressing a Denial of Service Vulnerability that exists in their products. **CVE-2023-52340** - The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/route.c max_size threshold that can be consumed easily, e.g., leading to a denial of service (network is unreachable errors) when IPv6 packets are sent in a loop via a raw socket. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere versions 9.11, 9.12 and 9.13. E-Series SANtricity OS Controller Software versions 11.70.5 and 11.80GA
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240816-0005/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure , memory corruption, system crash. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 openSUSE Leap Micro 5.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243209-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20304, CVE-2024-20381, CVE-2024-20317, CVE-2024-20406, CVE-2024-20398, CVE-2024-20483, CVE-2024-20489, CVE-2024-20390, CVE-2024-20343)
Description	Cisco 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, Privilege Escalation, Command Injection and Information Disclosure. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco IOS XR versions 6.7.4 and earlier, 7.11 and earlier, 24.1, 24.2 ConfD versions 7.5 through 7.5.10.1, 7.7 through 7.7.15, 8.0 through 8.0.12 Crosswork NSO 5.5, 5.6, 5.7, 5.8, 6.0, 6.1, 6.2 Cisco Optical Site Manager versions 24.3 and earlier Cisco Routed PON Controller Software in Cisco IOS XR 24.1 and later, 24.2 and later, 24.3 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pak-mem-exhst-3ke9FeFy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-l2services-2mvHdNuC • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-xehpbVNe • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-CrG5vhCq • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ponctlr-ci-OHcHmsFL • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-xml-tcpdos-ZEXvrU2S • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-shellutil-HCb278wD

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1012, CVE-2022-32296, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166, CVE-2024-38483)
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 system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Avamar Data Store Switch S4128F version 10.5.4.1 Multiple products that use Dell Client Platform BIOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000228478/dsa-2024-394-security-update-for-dell-avamar-security-update-for-switch-os-10-5-x-gen5a-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225776/dsa-2024-260-security-update-for-dell-client-platform-bios-for-an-improper-input-validation-vulnerability

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-8686, CVE-2024-8687, CVE-2024-8688, CVE-2024-8689, CVE-2024-8690, CVE-2024-8691)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Command Injection, Information Disclosure, Impersonation attacks. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2.2 PAN-OS 11.0 versions prior to 11.0.1 PAN-OS 10.2 versions prior to 10.2.4 PAN-OS 10.1 versions prior to 10.1.11 PAN-OS 10.0 versions prior to 10.0.12 PAN-OS 9.1 versions prior to 9.1.17 PAN-OS 9.0 versions prior to 9.0.17 PAN-OS 8.1 versions prior to 8.1.25 Prisma Access versions prior 10.2.9 on PAN-OS GlobalProtect App 6.2 versions prior to 6.2.1 GlobalProtect App 6.1 versions prior to 6.1.2 GlobalProtect App 6.0 versions prior to 6.0.7 GlobalProtect App 5.2 versions prior to 5.2.13 GlobalProtect App 5.1 versions prior to 5.1.12 ActiveMQ Content Pack 1.1 versions prior to 1.1.15 All versions of Cortex XDR Agent 7.9.102-CE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-8686 • https://security.paloaltonetworks.com/CVE-2024-8687 • https://security.paloaltonetworks.com/CVE-2024-8688 • https://security.paloaltonetworks.com/CVE-2024-8689 • https://security.paloaltonetworks.com/CVE-2024-8690 • https://security.paloaltonetworks.com/CVE-2024-8691

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6874, CVE-2024-6197, CVE-2024-5535, CVE-2024-7264, CVE-2024-6119)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Wincollect component. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, abnormal behaviour. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar WinCollect Agent versions 10.0 - 10.1.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7168115

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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6999-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52463, CVE-2023-52801, CVE-2024-26629, CVE-2024-26630, CVE-2024-26720, CVE-2024-26886, CVE-2024-26946, CVE-2024-35791, CVE-2024-35797, CVE-2024-35875, CVE-2024-36000, CVE-2024-36019, CVE-2024-36883, CVE-2024-36979, CVE-2024-38559, CVE-2024-38619, CVE-2024-40927, CVE-2024-40936, CVE-2024-41040, CVE-2024-41044, CVE-2024-41055, CVE-2024-41073, CVE-2024-41096, CVE-2024-42082, CVE-2024-42096, CVE-2024-42102, CVE-2024-42131)
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 for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x 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 Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:6567

Affected Product	**Drupal**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure and Denial of Service conditions. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	File Eentity versions prior to 7.x-2.39 for Drupal 7 Security Kit versions prior to both 7.x-1.13 and 2.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-040 • https://www.drupal.org/sa-contrib-2024-039

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.