Advisory Alert

Alert Number: AAA20250916 **Date:** September 16, 2025

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**, **Medium**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**High**, **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 affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	CyberSense software OVA (build 8.13.0-1.9) Versions - prior to 8.13 PowerProtect Cyber Recovery Software Versions - prior to 19.20.0.1 PowerProtect Cyber Recovery SLES 15 SP4 OS Update Versions - prior to 15.4.0-9 PowerProtect Cyber Recovery Osupdate 15.4.0-9.bin Versions - prior to 15.4.0-9 PowerProtect Cyber Recovery SLES 12 SP5 OS Update Versions - prior to 1.5.0-63 PowerProtect Cyber Recovery Osupdate 1.5.0-63.bin Versions - prior to 1.5.0-63
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000369848/dsa-2025-344-security-update-for-dell-cybersense-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000369807/dsa-2025-346-security-update-for-dell-powerprotect-cyber-recovery-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21659, CVE-2025-21701, CVE-2025-21999, CVE-2025-37890, CVE-2025-38000, CVE-2025-38001, CVE-2025-38087, CVE-2025-38212, CVE-2024-47674, CVE-2024-47706, CVE-2024-49867)
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 15.6 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 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503217-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503221-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503222-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503223-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38350, CVE-2025-38392, CVE-2025-38449, CVE-2025-38052, CVE-2025-38352, CVE-2025-22068, CVE-2025-38332, CVE-2025-38463, CVE-2025-38498, CVE-2025-38500, CVE-2025-38550)
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 affected systems. 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 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:15782 • https://access.redhat.com/errata/RHSA-2025:15786 • https://access.redhat.com/errata/RHSA-2025:15798

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-50102, CVE-2025-50093, CVE-2025-50085, CVE-2025-50083, CVE-2025-50084, CVE-2025-50096, CVE-2025-50080, CVE-2025-50097, CVE-2025-50101, CVE-2025-50099, CVE-2025-50082, CVE-2025-50077, CVE-2025-50092, CVE-2025-5399, CVE-2025-50100, CVE-2025-50078, CVE-2025-50104, CVE-2025-50091, CVE-2025-50098, CVE-2025-50087, CVE-2025-50079, CVE-2025-50086)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause sensitive information disclosure, denial of service, addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SnapCenter OnCommand Insight NetApp Service Level Manager SnapCenter Plug-in for VMware vSphere/BlueXP Backup and Recovery for Virtual Machine
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250725-0005 • https://security.netapp.com/advisory/ntap-20250724-0008

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20613, CVE-2025-22853, CVE-2025-21096, CVE-2025-20053, CVE-2025-24305, CVE-2025-21090, CVE-2025-24486, CVE-2025-25273, CVE-2025-21086, CVE-2025-26863, CVE-2025-26697, CVE-2025-24511)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause disclosure of information, escalation of privilege and denial of service. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110, 4120, 4140 - Prior to 2.60_08-07-2025 HPE Alletra Storage Server 4210 - Prior to 1.50_09-05-2025 HPE Compute Edge Server e930t - Prior to 2.60_08-07-2025 HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - Prior to 2.28.5 HPE Ethernet 10Gb 2-port 562SFP+ Adapter - Prior to 2.28.5 HPE Ethernet 10Gb 2-port 563i Adapter - Prior to 2.28.5 HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter - Prior to 2.28.5 HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter - Prior to 2.28.5 HPE Ethernet 10Gb 2-port 568i Adapter - Prior to 2.28.5 HPE Ethernet 1Gb 2-port 361i Adapter - Prior to 5.19.2 HPE Ethernet 1Gb 2-port 361T Adapter - Prior to 5.19.2 HPE Ethernet 1Gb 2-port 363i Adapter - Prior to 5.19.2 HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter - Prior to 2.28.5 HPE Ethernet 1Gb 2-port 368i Adapter - Prior to 2.28.5 HPE Ethernet 1Gb 4-port 366FLR Adapter - Prior to 5.19.2 HPE Ethernet 1Gb 4-port 366i Adapter - Prior to 5.19.2 HPE Ethernet 1Gb 4-port 366i Communication Board - Prior to 5.19.2 HPE Ethernet 1Gb 4-port 366T Adapter - Prior to 5.19.2, 369i Adapter - Prior to 2.28.5 HPE ProLiant Compute DL320 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL340 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL360 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL380 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL380a Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL384 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL580 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute ML350 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute XD230 - Prior to 1.50_09-05-2025 HPE ProLiant DL110 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant DL320 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL360 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL380 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL380a Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant DL560 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant ML110 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant ML350 Gen11 Server - Prior to 2.60_08-07-2025 HPE Synergy 480 Gen11 Compute Module - Prior to 2.60_08-07-2025 Intel I350-T4 Ethernet 1Gb 4-port BASE-T Adapter for HPE - Prior to 5.19.2 Intel I350-T4 Ethernet 1Gb 4-port BASE-T OCP3 Adapter for HPE - Prior to 5.19.2 Intel X710-DA2 Ethernet 10Gb 2-port SFP+ Adapter for HPE - Prior to 2.28.5 Intel X710-DA2 Ethernet 10Gb 2-port SFP+ OCP3 Adapter for HPE - Prior to 2.28.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04916en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04917en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04919en_us&docLocale=en_US

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.