Advisory Alert

Alert Number: **AAA20250924** **Date:** **September 24, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Authentication Bypass Vulnerability
Oracle	**Critical**	Use After Free Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
IBM	**High**	Denial of Service Vulnerability
NetApp	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Buffer Overflow Vulnerability
Oracle	**High, Medium**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-3596)
Description	HPE has released security updates addressing an authentication bypass vulnerability that exists in their products. **CVE-2024-3596 -** The attacker must have man-in-the-middle access between the RADIUS client and server and the ability to trigger an Access-Request. By predicting the Access-Reject response and computing an MD5 chosen-prefix collision (within 5 to 6 minutes, potentially faster with more resources), the attacker can modify the client request, remove any Message-Authenticator attributes if PAP authentication is used, and forge an Access-Accept response by copying the Response Authenticator from the Access-Reject response. This modified response, when sent to the client, grants the attacker unauthorized access to resources authenticated/authorized via RADIUS. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Aruba AirWave Management Platform See Vulnerability Summary • Aruba ClearPass Policy Manager Platform See Vulnerability Summary • ArubaOS SD-WAN Gateways See Vulnerability Summary • ArubaOS Wi-Fi Controllers and Gateways See Vulnerability Summary • Aruba CX 10000, CX 4100i, CX 6000, CX 6100, CX 6200F, CX 6300, CX 8320, CX 8325, CX 8360, CX 8400, CX 9300 Switch Series See Vulnerability Summary • Aruba EdgeConnect Enterprise Orchestration Software See Vulnerability Summary • Aruba EdgeConnect Enterprise Software See Vulnerability Summary • Aruba 100, 103, 110, 120, 130, 200, 207, 210, 220, 260, 300, 303, 310, 320, 330, 340, 370, 500, 510, 530, 550, 630, 650 Series Access Points See Vulnerability Summary
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04662en_us&docLocale=en_US

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Use After Free Vulnerability (CVE-2025-6424)
Description	Oracle has released security updates addressing a use after free vulnerability that exists third party components, which in turn affects their products. **CVE-2025-6424 -** A use-after-free in FontFaceSet resulted in a potentially exploitable crash. This vulnerability affects Firefox < 140, Firefox ESR < 115.25, Firefox ESR < 128.12, Thunderbird < 140, and Thunderbird < 128.12. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris thunderbird
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjul2025.html

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	• Data Protection Central OS Update (SUSE SLES 12 SP5) - Version 19.8 through 19.12 with Data Protection Central OS Update prior to dpc-osupdate-1.1.24-1 • PowerProtect DP Series (Integrated Data Protection Appliance (IDPA) Appliance) Data Protection Central OS Update for Power Protect DP Series Appliances - Version 2.7.9 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000372522/dsa-2025-361-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37890, CVE-2025-38000, CVE-2025-38001, CVE-2025-38350, CVE-2025-38380)
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 Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64, AUS 9.4 x86_64, AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:16538 • https://access.redhat.com/errata/RHSA-2025:16539 • https://access.redhat.com/errata/RHSA-2025:16540 • https://access.redhat.com/errata/RHSA-2025:16541

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing multiple Linux Kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6, Development Tools Module 15-SP6, Legacy Module 15-SP6 OpenSUSE Leap 15.3, 15.4, 15.6, SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP3, 15 SP4, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, LTSS 15 SP3, LTSS 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP6 SUSE Linux Enterprise Server 15 SP3, Business Critical Linux, SP3 LTSS, SP4, SP4 LTSS, SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Manager Proxy 4.2, 4.3, 4.3 LTS SUSE Manager Retail Branch Server 4.2, 4.3, 4.3 LTS SUSE Manager Server 4.2, 4.3, 4.3 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503301-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503310-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503314-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-30204)
Description	IBM has released security updates addressing a denial of service vulnerability that exists in their products. **CVE-2025-30204 -** golang-jwt is a Go implementation of JSON Web Tokens. Starting in version 3.2.0 and prior to versions 5.2.2 and 4.5.2, the function parse.ParseUnverified splits (via a call to strings.Split) its argument (which is untrusted data) on periods. As a result, in the face of a malicious request whose Authorization header consists of Bearer followed by many period characters, a call to that function incurs allocations to the tune of O(n) bytes (where n stands for the length of the function's argument), with a constant factor of about 16. This issue is fixed in 5.2.2 and 4.5.2. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale Versions - 5.1.9.0 - 5.1.9.11 IBM Storage Scale Versions - 5.2.1.0 - 5.2.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7245948

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32415, CVE-2024-8176, CVE-2025-27113, CVE-2024-55549, CVE-2024-56171, CVE-2025-24928, CVE-2025-1736, CVE-2024-11168, CVE-2025-1219, CVE-2025-1734, CVE-2025-1861, CVE-2024-6923, CVE-2025-26466, CVE-2025-1217)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause addition or modification of data, denial of service, authentication bypass and sensitive information disclosure. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250605-0003 • https://security.netapp.com/advisory/ntap-20250328-0009 • https://security.netapp.com/advisory/ntap-20250306-0004 • https://security.netapp.com/advisory/ntap-20250613-0007 • https://security.netapp.com/advisory/ntap-20250328-0010 • https://security.netapp.com/advisory/ntap-20250321-0006 • https://security.netapp.com/advisory/ntap-20250523-0006 • https://security.netapp.com/advisory/ntap-20250411-0004 • https://security.netapp.com/advisory/ntap-20250523-0007 • https://security.netapp.com/advisory/ntap-20250523-0009 • https://security.netapp.com/advisory/ntap-20250523-0005 • https://security.netapp.com/advisory/ntap-20240926-0003 • https://security.netapp.com/advisory/ntap-20250228-0002 • https://security.netapp.com/advisory/ntap-20250523-0008

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2025-37122, CVE-2025-37123, CVE-2025-37124, CVE-2025-37125, CVE-2025-37126, CVE-2025-37127, CVE-2025-37128, CVE-2025-37129, CVE-2025-37130, CVE-2025-37131)
Description	HPE has released security updates addressing a buffer overflow vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 prior to v1.60.88 HPE Superdome Flex Server prior to v4.10.18 HPE Superdome Flex 280 Server prior to v2.05.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04857en_us&docLocale=en_US

Affected Product	**Oracle**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-4674, CVE-2025-58060, CVE-2025-21086, CVE-2025-49630, CVE-2025-47907, CVE-2025-24294, CVE-2025-50078, CVE-2025-8027, CVE-2025-54090, CVE-2025-6491, CVE-2024-36348)
Description	Oracle has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris Go Programming Language Oracle Solaris Common Unix Printing System (CUPS) Oracle Solaris Apache HTTP server Oracle Solaris Go Programming Language Oracle Solaris Apache HTTP server Oracle Solaris Firefox Oracle Solaris PHP Oracle Solaris Kernel Oracle Solaris Ruby Oracle Solaris MySQL Oracle Solaris Driver
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjul2025.html

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-43943, CVE-2025-26482)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-43943 -** Dell Cloud Disaster Recovery, version(s) prior to 19.20, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges. **CVE-2025-26482 -** Dell PowerEdge Server BIOS and Dell iDRAC9, all versions, contains an Information Disclosure vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information Disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000372457/dsa-2025-354-security-update-for-dell-cloud-disaster-recovery-rce-vulnerability • https://www.dell.com/support/kbdoc/en-us/000370138/dsa-2025-046-security-update-for-dell-poweredge-server-and-dell-idrac9-for-information-disclosure-vulnerability

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.