Advisory Alert

Alert Number: **AAA20251001** **Date:** **October 1, 2025**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Palo Alto Networks	**Medium**	Privilege Escalation Vulnerability
OpenSSL	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical - Initial release date 9th April 2025 (AAA20250409)**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-2961, CVE-2024-52533, CVE-2023-6780)
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 iDRAC9 - Versions prior to 7.00.00.181 Dell iDRAC9 - Versions prior to 7.20.30.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000299628/dsa-2025-146-security-update-for-dell-idrac9-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20044, CVE-2025-20109, CVE-2024-33607)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-20044 -** Improper locking for some Intel TDX Module firmware before version 1.5.13 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE-2025-20109 -** Improper Isolation or Compartmentalization in the stream cache mechanism for some Intel Processors may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE-2024-33607 -** A potential security vulnerability in some Intel Trust Domain Extensions (Intel TDX) module software may allow information disclosure. Intel is releasing firmware updates to mitigate this potential vulnerability. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Precision 7960 Rack BIOS - Versions prior to 2.7.5 Dell Precision 7960 XL Rack BIOS - Versions prior to 2.7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000331788/dsa-2025-240

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22058, CVE-2025-22097, CVE-2025-38477, CVE-2022-48701,CVE-2022-50211, CVE-2022-50229, CVE-2023-53125, CVE-2025-38200, CVE-2025-37810, CVE-2025-38449, CVE-2025-38461, CVE-2025-38472, CVE-2025-38527, CVE-2025-21759)
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 Real Time for x86_64 - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64, TUS 8.6 x86_64, TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17009 • https://access.redhat.com/errata/RHSA-2025:17109 • https://access.redhat.com/errata/RHSA-2025:17123 • https://access.redhat.com/errata/RHSA-2025:17124

Affected Product	**Palo Alto Networks**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-0117)
Description	Palo Alto Networks has released security update addressing a privilege escalation vulnerability that exists in their products. **CVE-2025-0117 -** A reliance on untrusted input for a security decision in the GlobalProtect app on Windows devices potentially enables a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY\SYSTEM. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Palo Alto Networks GlobalProtect App 6.3 - Versions prior to 6.3.3 on Windows Palo Alto Networks GlobalProtect App 6.2 - Versions prior to 6.2.6 on Windows Palo Alto Networks GlobalProtect App 6.1 - All Versions on Windows Palo Alto Networks GlobalProtect App 6.0 - Versions prior to 6.0.12 on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2025-0117

Affected Product	**OpenSSL**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9230, CVE-2025-9231, CVE-2025-9232)
Description	OpenSSL has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-9230 -** This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. **CVE-2025-9231 -** A timing side-channel which could potentially allow remote recovery of the private key exists in the SM2 algorithm implementation on 64 bit ARM platforms. **CVE-2025-9232 -** An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SM2 algorithm on 64 bit ARM • from 3.5.0 before 3.5.4 • from 3.4.0 before 3.4.3 • from 3.3.0 before 3.3.5 • from 3.2.0 before 3.2.6 HTTP client no_proxy handling • from 3.5.0 before 3.5.4 • from 3.4.0 before 3.4.3 • from 3.3.3 before 3.3.5 • from 3.2.4 before 3.2.6 • from 3.0.16 before 3.0.18 RFC 3211 KEK Unwrap • from 3.5.0 before 3.5.4 • from 3.4.0 before 3.4.3 • from 3.3.0 before 3.3.5 • from 3.2.0 before 3.2.6 • from 3.0.0 before 3.0.18 • from 1.1.1 before 1.1.1zd • from 1.0.2 before 1.0.2zm
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/

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.