Advisory Alert

Alert Number: **AAA20250714** **Date:** **July 14, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Lenovo	**Medium**	Out-of-Bounds Read Vulnerability
Apache HTTP Server	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0150, CVE-2024-0147, CVE-2024-0131, CVE-2025-30483)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000261121/dsa-2025-030 • https://www.dell.com/support/kbdoc/en-us/000339124/dsa-2025-242-security-update-for-dell-ecs-and-dell-objectscale-insertion-of-sensitive-information-into-log-file-vulnerability

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21991, CVE-2022-49846, CVE-2022-50066, CVE-2022-49395, CVE-2022-49122, CVE-2025-21759, CVE-2023-52933, CVE-2025-22004, CVE-2025-22121, CVE-2025-22104, CVE-2025-37738, CVE-2022-49328)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:10837 • https://access.redhat.com/errata/RHSA-2025:10834 • https://access.redhat.com/errata/RHSA-2025:10830 • https://access.redhat.com/errata/RHSA-2025:10829 • https://access.redhat.com/errata/RHSA-2025:10828

Affected Product	**Lenovo**
Severity	**Medium**
Affected Vulnerability	Out-of-Bounds Read Vulnerability (CVE-2025-2884)
Description	Lenovo has released a security update to address an Out-of-Bounds Read vulnerability that exists in their products. This vulnerability could be exploited by malicious users to cause information disclosure and denial-of-service. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-165940

Affected Product	**Apache HTTP Server**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42516, CVE-2024-43204, CVE-2024-43394, CVE-2024-47252, CVE-2025-23048, CVE-2025-49630, CVE-2025-49812, CVE-2025-53020, CVE-2023-38709)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause HTTP response splitting, server-side request forgery, denial-of-service attacks. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server: from 2.4.0 up to 2.4.63 All versions prior to 2.4.63 if SSLEngine optional configuration enabled
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.