Advisory Alert

Alert Number: AAA20250221 **Date:** February 21, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Lenovo	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**,	Multiple Vulnerabilities

Description

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20507, CVE-2023-20515, CVE-2023-20581, CVE-2023-20582, CVE-2023-31331, CVE-2023-31342, CVE-2023-31343, CVE-2023-31345, CVE-2023-31352, CVE-2023-34440, CVE-2023-43758, CVE-2023-45236, CVE-2023-45237, CVE-2023-48267, CVE-2023-48366, CVE-2023-49603, CVE-2023-49615, CVE-2023-49618, CVE-2024-0179, CVE-2024-1298, CVE-2024-20214, CVE-2024-21859, CVE-2024-21924, CVE-2024-21925, CVE-2024-24582, CVE-2024-25571, CVE-2024-28047, CVE-2024-28127, CVE-2024-31068, CVE-2024-31155, CVE-2024-31157, CVE-2024-33659, CVE-2024-36262, CVE-2024-36293, CVE-2024-37020, CVE-2024-39279, CVE-2024-39355, CVE-2024-49199, CVE-2024-56161, CVE-2024-21971, CVE-2023-20508)
Description	Lenovo has released security updates addressing Multiple Vulnerabilities that exist in their products. Lenovo has identified multiple security vulnerabilities affecting BIOS firmware in various products. Exploitation of these flaws could enable attackers to execute arbitrary code or gain elevated privileges. Immediate firmware updates are required to mitigate risks. (CVE-2024-21971, CVE-2023-20508) Lenovo has identified multiple security vulnerabilities in AMD graphics drivers that could allow attackers to escalate Privilege escalation, information disclosure, and denial of system security. Update AMD graphics drivers immediately via Lenovo's official update. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Multiple Lenovo ThinkPad • ThinkCentre • ThinkStation • IdeaPad • Legion models
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.lenovo.com/us/en/product_security/LEN-186850 • https://support.lenovo.com/us/en/product_security/LEN-179277

Affected Product	**DELL**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56161, CVE-2024-38796)
Description	DELL has identified multiple security vulnerabilities affecting BIOS firmware in Dell PowerEdge Servers. Exploitation of these flaws could enable attackers to compromise affected systems. Immediate firmware updates are required to mitigate risks 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/000280550/dsa-2025-040-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000287202/dsa-2025-038-security-update-for-dell-poweredge-server-bios-for-tianocore-edk2-vulnerability

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21538, CVE-2024-21536, CVE-2023-29019, CVE-2023-29020, CVE-2024-28047, CVE-2024-39279, CVE-2024-31157)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. (CVE-2024-21538, CVE-2024-21536, CVE-2023-29019, CVE-2023-29020) Potential security vulnerabilities have been identified in HPE Telco Service Orchestrator software. These vulnerabilities could be remotely exploited to allow cross-site request forgery, elevation of privilege, and denial of service. (CVE-2024-28047, CVE-2024-39279, CVE-2024-31157) Security vulnerabilities in HPE ProLiant DL/ML/XL Alletra, Edgeline and Synergy products for certain Intel processors could be locally exploited to allow disclosure of information, and denial of service. For more information on these vulnerabilities, please see Intel Security Advisory INTEL-SA-01139, 2025.1 IPU - UEFI Firmware Advisory. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Telco Service Orchestrator v5.1.2 or later HPE Alletra 4110 - Prior to v2.44_01-17-2025 HPE Alletra 4120 - Prior to v2.44_01-17-2025 HPE Alletra 4140 - Prior to v2.44_01-17-2025 HPE ProLiant DL110 Gen11 - Prior to v2.44_01-17-2025 HPE ProLiant DL320 Gen11 Server - Prior to v2.44_01-17-2025 HPE ProLiant DL360 Gen11 Server - Prior to v2.44_01-17-2025 HPE ProLiant DL380 Gen11 Server - Prior to v2.44_01-17-2025 HPE ProLiant DL380a Gen11 - Prior to v2.44_01-17-2025 HPE ProLiant DL560 Gen11 - Prior to v2.44_01-17-2025 HPE ProLiant ML110 Gen11 - Prior to v2.44_01-17-2025 HPE ProLiant ML350 Gen11 Server - Prior to v2.44_01-17-2025 HPE Synergy 480 Gen11 Compute Module - Prior to v2.44_01-17-2025 HPE Compute Edge Server e930t - Prior to v2.44_01-17-2025 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.30_01-16-2025 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.30_01-16-2025 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.30_01-16-2025 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.30_01-16-2025 HPE Apollo 2000 Gen10 Plus System - Prior to v2.30_01-16-2025 HPE Apollo 4200 Gen10 Plus System - Prior to v2.30_01-16-2025 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.30_01-16-2025 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.30_01-16-2025 HPE Edgeline e920 Server Blade - Prior to v2.30_01-16-2025 HPE Edgeline e920d Server Blade - Prior to v2.30_01-16-2025 HPE Edgeline e920t Server Blade - Prior to v2.30_01-16-2025 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.40_01-16-2025 HPE Synergy 480 Gen10 Compute Module - Prior to v3.40_01-16-2025 HPE Synergy 660 Gen10 Compute Module - Prior to v3.40_01-16-2025 HPE Apollo 2000 System - Prior to v3.40_01-16-2025 HPE Apollo 4200 Gen10/HPE ProLiant XL420 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant XL190r Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant XL170r Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant e910 Server Blade - Prior to v3.40_01-16-2025 HPE ProLiant e910t Server Blade - Prior to v3.40_01-16-2025 HPE ProLiant DL120 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL160 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL180 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL360 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL380 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL560 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL580 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant ML110 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant ML350 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant MicroServer Gen10 - Prior to v3.50_01-16-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04768en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04790en_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.