Advisory Alert

Alert Number: AAA20260901 **Date:** September 1, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
HPE	**Medium**	Information Disclosure Vulnerability

Description

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414, CVE-2026-46333)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell OpenManage Network Integration Versions prior to 3.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000504800/dsa-2026-289-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

Vendor	**HPE**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2026-20917)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-20917**: A potential security vulnerability in HPE ProLiant DL/ML/XL, Apollo, Edgeline, MicroServer and Synergy servers using certain Intel processors could be locally exploited to allow disclosure of information vulnerability. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE ProLiant DL20 Gen10 Plus server - prior to v2.70_08-20-2026 • HPE ProLiant DL110 Gen10 Plus Telco server - prior to v2.70_08-19-2026 • HPE ProLiant DL360 Gen10 Plus server - prior to v2.70_08-19-2026 • HPE ProLiant DL380 Gen10 Plus server - prior to v2.70_08-19-2026 • HPE ProLiant MicroServer Gen10 Plus v2 - prior to v2.70_08-20-2026 • HPE ProLiant ML30 Gen10 Plus server - prior to v2.70_08-20-2026 • HPE Synergy 480 Gen10 Plus Compute Module - prior to v2.70_08-19-2026 • HPE Apollo 2000 Gen10 Plus System - prior to v2.70_08-19-2026 • HPE Apollo 4200 Gen10 Plus/HPE ProLiant XL420 Gen10 Plus Server - prior to v2.70_08-19-2026 • HPE ProLiant XL220n Gen10 Plus Server - prior to v2.70_08-19-2026 • HPE ProLiant XL290n Gen10 Plus Server - prior to v2.70_08-19-2026 • HPE Edgeline e920 Server Blade - prior to v2.70_08-19-2026 • HPE Edgeline e920d Server Blade - prior to v2.70_08-19-2026 • HPE Edgeline e920t Server Blade - prior to v2.70_08-19-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05127en_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.