Advisory Alert

Alert Number: AAA20260316 **Date:** March 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
HP	**High**	Privilege Escalation Vulnerability
OpenSSL	**Low**	Security Update

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20044, CVE-2024-43420, CVE-2024-45332, CVE-2025-20109)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the third-party Intel component, utilized by 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	PowerSwitch Z9664F-ON Firmware versions prior to 3.54.5.1-11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000439031/dsa-2026-138-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-4000)
Description	HP has released a security update addressing a vulnerability that exists in their Hotkey UWP Service. **CVE-2026-4000**: This vulnerability, if exploited can lead to a successful escalation of privilege. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_14484164-14484183-16/hpsbhf04102

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Security Update (CVE-2026-2673)
Description	OpenSSL has released a security update addressing a vulnerability that exists in their products. **CVE-2026-2673**: An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group configuration includes the default by using the 'DEFAULT' keyword. OpenSSL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSSL versions 3.6.0 to but not including 3.6.2 OpenSSL versions 3.5.0 to but not including 3.5.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/#CVE-2026-2673

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.