Advisory Alert

Alert Number: AAA20251219 **Date:** December 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WatchGuard	**Critical**	Out of Bounds Write Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
F5	**High**	Path Traversal Vulnerability
Dell	**High, Medium**	Multiple Vulnerabilities
PHP	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Out of Bounds Write Vulnerability (CVE-2025-14733)
Description	WatchGuard has released a security update addressing an out of bounds write vulnerability that is present in Fireware OS. **CVE-2025-14733:** An Out-of-bounds Write vulnerability in the WatchGuard Fireware OS iked process may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the mobile user VPN with IKEv2 and the branch office VPN using IKEv2 when configured with a dynamic gateway peer. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS versions: • 11.10.2 up to and including 11.12.4_Update1 • 12.0 up to and including 12.11.5 • 2025.1 up to and including 2025.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third-party components present in Dell Metro node. 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	Metro node mn-114 versions prior to 9.1.0.0 Metro node mn-115 versions prior to 9.1.0.0 Metro node mn-216 versions prior to 9.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000405301/dsa-2025-452-security-update-for-dell-metro-node-multiple-third-party-component

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2025-14727)
Description	F5 has released a security update addressing a path traversal vulnerability that exists within the NGINX Ingress Controller. **CVE-2025-14727:** A vulnerability exists in the NGINX Ingress Controller nginx.org/rewrite-target annotation validation. This vulnerability may allow an authenticated attacker with ingress creation privileges to inject arbitrary NGINX configuration directives, potentially leading to information disclosure, privilege escalation, and service disruption. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NGINX Ingress Controller version 5.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000158176

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42446, CVE-2023-38709, CVE-2025-46802, CVE-2025-46805, CVE-2025-7425, CVE-2025-7424, CVE-2025-43723, CVE-2025-46429, CVE-2025-46431)
Description	Dell has released a security update addressing multiple vulnerabilities that are present 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000405391/dsa-2025-370-security-update-for-dell-poweredge-server-for-a-toctou-vulnerability • https://www.dell.com/support/kbdoc/en-us/000390206/dsa-2025-381-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities

Affected Product	**PHP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-14180, CVE-2025-14178, CVE-2025-14177)
Description	PHP has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-14180**: A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. **CVE-2025-14178:** PHP array_merge() can overflow when merging many arrays due to an integer overflow in element count calculation, leading to heap corruption or denial of service when processing attacker-controlled data. **CVE-2025-14177:** The application insufficiently controls access to information processed by the application data caching tool. As a result, an attacker can gain access to cached data. PHP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PHP versions prior to: • 8.1.34 • 8.2.30 • 8.3.29 • 8.4.16 • 8.5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php

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.