Advisory Alert

Alert Number: AAA20250321 **Date:** March 21, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
FortiGuard	**High**	Multiple Path Traversal Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26336, CVE-2018-18065, CVE-2018-1000116)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in Dell PowerEdge CMC. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2 Versions prior to 2.40.200.202101130302 • Dell Chassis Management Controller (CMC) for PowerEdge VRTX Versions prior to 3.41.200.202209300499
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000297463/dsa-2025-123-security-update-for-dell-chassis-management-controller-firmware-for-dell-poweredge-fx2-and-vrtx-vulnerabilities

Affected Product	**FortiGuard**	
Severity	**High**	
Affected Vulnerability	Multiple Path Traversal Vulnerabilities (CVE-2024-48884 ,CVE-2024-48885)	
Description	FortiGuard has released security updates addressing multiple Path Traversal Vulnerabilities that exist in their products. An improper limitation of a pathname to a restricted directory vulnerability ('path traversal') in FortiManager, FortiOS, FortiProxy, FortiRecorder, FortiVoice and FortiWeb may allow a remote authenticated attacker with access to the security fabric interface and port to write arbitrary files and a remote unauthenticated attacker with the same network access to delete an arbitrary folder. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiManager 7.6.0 through 7.6.1 FortiManager 7.4.1 through 7.4.3 FortiManager Cloud 7.4.1 through 7.4.3 FortiOS 7.6.0 FortiOS7.4.0 through 7.4.4 FortiOS 7.2.0 through 7.2.9 FortiOS 7.0.0 through 7.0.15 FortiOS 6.4.0 through 6.4.15 FortiProxy 7.4.0 through 7.4.5 FortiProxy 7.2.0 through 7.2.11 FortiProxy 7.0.0 through 7.0.18	FortiRecorder 7.2.0 through 7.2.1 FortiRecorder 7.0.0 through 7.0.4 FortiVoice 7.0.0 through 7.0.4 FortiVoice 6.4.0 through 6.4.9 FortiVoice 6.0 all versions FortiWeb 7.6.0 FortiWeb 7.4.0 through 7.4.4 FortiWeb 7.2 all versions FortiWeb 7.0 all versions FortiWeb 6.4 all versions
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-24-259	

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.