Advisory Alert

Alert Number: **AAA20250423** **Date:** **April 23, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Plain-Text Password Storage Vulnerability
Synology	**High**	Missing Authorization Vulnerability
HPE	**High , Medium**	Multiple Vulnerabilities
Fortiguard	**High , Medium**	Multiple Vulnerabilities
IBM	**Medium**	Server-Side Request Forgery Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Plain-text password storage vulnerability (CVE-2019-3753)
Description	Dell has released security updates addressing a plain-text password storage vulnerability in Dell PowerConnect 8024, 7000, M6348, M6220, M8024, and M8024-K running firmware versions prior to 5.1.15.2.TACACS/RADIUS credentials are stored in plain text within the system settings menu. An authenticated, malicious user with access to this menu may obtain the exposed credentials and use them in further attacks. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC PowerConnect models running firmware versions prior to 5.1.15.2: • 8024 • 7000 • M6348 • M6220 • M8024 • M8024-K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000125969/dsa-2019-124-dell-emc-powerconnect-security-vulnerability

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Missing authorization vulnerability (CVE-2025-1021)
Description	Synology has released security updates addressing a Missing authorization vulnerability in Synology DiskStation Manager (DSM) before 7.1.1-42962-8, 7.2.1-69057-7 and 7.2.2-72806-3 allows remote attackers to read arbitrary files via unspecified vectors. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology DSM 7.2.2 versions prior to 7.2.2-72806-3 Synology DSM 7.2.1 versions prior to 7.2.1-69057-7 Synology DSM 7.1 versions prior to 7.1.1-42962-8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_03

Affected Product	**HPE**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7344, CVE-2024-23593, CVE-2024-23594, CVE-2024-28924, CVE-2025-1976)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Unauthorized Arbitrary File Creation, Bypass Security Restrictions, Code Execution, and Escalation of Privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - Prior to v1.55.98 HPE Superdome Flex 280 Server - Prior to v2.00.12 HPE Brocade Fabric OS - Prior to v9.1.1d7 and v9.2.0 - (v9.1.0 through 9.1.1d6 are affected)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04830en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04846en_us&docLocale=en_US

Affected Product	**Fortiguard**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26013, CVE-2024-50565, CVE-2024-50570)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-26013, CVE-2024-50565 -** A improper restriction of communication channel to intended endpoints vulnerability in FortiOS, FortiProxy, FortiManager, FortiAnalyzer, FortiVoice and FortiWeb may allow an unauthenticated attacker in a man-in-the-middle position to impersonate the management device (FortiCloud server or/and in certain conditions, FortiManager), via intercepting the FGFM authentication request between the management device and the managed device **CVE-2024-50570 -** A Cleartext Storage of Sensitive Information vulnerability in FortiClient Windows and FortiClient Linux may permit a local authenticated user to retrieve VPN password via memory dump, due to JavaScript's garbage collector Fortiguard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAnalyzer 7.4.0 through 7.4.2 FortiAnalyzer 7.2.0 through 7.2.4 FortiAnalyzer 7.0.0 through 7.0.11 FortiAnalyzer 6.4.0 through 6.4.14 FortiAnalyzer 6.2.0 through 6.2.13 FortiManager 7.4.0 through 7.4.2 FortiManager 7.2.0 through 7.2.4 FortiManager 7.0.0 through 7.0.11 FortiManager 6.4.0 through 6.4.14 FortiManager 6.2.0 through 6.2.13 FortiOS 7.4.0 through 7.4.4 FortiOS 7.2.0 through 7.2.8 FortiOS 7.0.0 through 7.0.15 FortiOS 6.4 (all versions) FortiProxy 7.4.0 through 7.4.2 FortiProxy 7.2.0 through 7.2.9 FortiProxy 7.0.0 through 7.0.15 FortiProxy 2.0 (all versions) FortiVoice 7.0.0 through 7.0.2 FortiVoice 6.4.0 through 6.4.8 FortiVoice 6.0 (all versions) FortiWeb 7.4.0 through 7.4.2 FortiClientLinux 7.4.0 through 7.4.2 FortiClientLinux 7.2.0 through 7.2.7 FortiClientLinux 7.0 (all versions) FortiClientWindows 7.4.0 through 7.4.1 FortiClientWindows 7.2.0 through 7.2.6 FortiClientWindows 7.0.0 through 7.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-046 • https://www.fortiguard.com/psirt/FG-IR-23-278

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Server-side request forgery Vulnerability (CVE-2025-27907)
Description	IBM has released a security update addressing a Server-Side Request Forgery (SSRF) vulnerability in IBM WebSphere Application Server. This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7231514

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.