TLP: WHITE

Advisory Alert

Alert Number: AAA20241028 **Date:** October 28, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
F5	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42898, CVE-2022-38023, CVE-2022-37966, CVE-2022-37967, CVE-2022-45141, CVE-2022-2031, CVE-2022-32742, CVE-2022-32744, CVE-2022-32745, CVE-2022-32746, CVE-2022-3592, CVE-2023-0614, CVE-2023-0225, CVE-2023-34968, CVE-2023-34967, CVE-2023-34966, CVE-2023-3347, CVE-2023-4091, CVE-2023-3961)
Description	HPE has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Compromise of System Integrity, Creation and Deletion of Arbitrary Files, Denial of Service, Directory Traversal, Elevation of Privilege, Gain Unauthorized Access HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX Common Internet File System (CIFS) Client/Server Software prior to B.04.18.01.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04724en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. 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 EMC VxRail Appliance Versions prior to 8.0.310
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000240575/dsa-2024-393-security-update-for-dell-vxrail-hci-8-0-310-multiple-third-party-component-vulnerabilities

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-10350, CVE-2016-10349, and CVE-2016-10209, CVE-2018-1000880, CVE-2019-1000020 ,CVE-2019-1000019, CVE-2024-6232)
Description	F5 has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service and compromise the affected system. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) 17.x Versions 17.1.0 - 17.1.1 BIG-IP (all modules) 16.x Versions 16.1.0 - 16.1.5 BIG-IP (all modules) 15.x Versions 15.1.0 - 15.1.10 BIG-IQ Centralized Management 8.x Versions 8.2.0 - 8.3.0 BIG-IP Next Central Manager 20.x Versions 20.2.0 - 20.2.1 BIG-IP Next SPK 1.x Versions 1.7.0 - 1.9.2 BIG-IP Next CNF 1.x Versions 1.1.0 - 1.3.1 F5OS-A 1.x 1.7.0 - 1.8.0 , 1.5.1 - 1.5.2 F5OS-C 1.x 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000148259 • https://my.f5.com/manage/s/article/K000148256 • https://my.f5.com/manage/s/article/K000148255 • https://my.f5.com/manage/s/article/K000148252

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.