Advisory Alert

Alert Number: AAA20250319 **Date:** March 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**High**	Multiple Buffer Overflows Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**FortiGuard**
Severity	**High**
Affected Vulnerability	Multiple Buffer Overflows Vulnerabilities (CVE-2021-22129)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their FortiNDR and FortiMail products. **CVE-2021-22129 -** Multiple instances of incorrect calculation of buffer size in FortiMail webmail and administrative interface and FortiNDR administrative interface may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiMail 6.4.4 and below FortiMail 6.2.6 and below FortiMail 6.0.10 and below FortiMail 5.4.12 and below FortiNDR 7.2.1 and below FortiNDR 7.1 all versions FortiNDR 7.0 all versions FortiNDR 1.5 all versions FortiNDR 1.4 all versions FortiNDR 1.3 all versions FortiNDR 1.2 all versions FortiNDR 1.1 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-023

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48792, CVE-2022-48911, CVE-2024-46818, CVE-2024-50302, CVE-2021-47261, CVE-2021-47496, CVE-2024-46815, CVE-2024-56648)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.1 - 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250893-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250896-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250897-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250898-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250904-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250903-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250906-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250907-1

Affected Product	**HPE**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-25040, CVE-2025-25042, CVE-2025-27080)
Description	HPE has released security updates addressing Multiple Vulnerabilities that exist in their Product. **CVE-2025-25040 -** A vulnerability in the AOS-CX software on HPE Aruba CX 9300 switches allows attackers to bypass port ACL rules on egress routed ports, potentially causing unauthorized traffic flow. Affected versions are AOS-CX 10.14.xxxx and 10.15.xxxx up to 10.15.1000. **CVE-2025-25042 -** A vulnerability in the AOS-CX REST interface could allow an authenticated remote attacker with low privileges to view sensitive information. Successful exploitation could allow an attacker to read encrypted credentials of other users on the switch, potentially leading to further unauthorized access or data breaches. **CVE-2025-27080 -** Vulnerabilities in the command line interface of AOS-CX could allow an authenticated remote attacker to expose sensitive information. Successful exploitation could allow an attacker to gain unauthorized access to services outside of the impacted switch, potentially leading to lateral movement involving those services. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Aruba CX 10000 Switch Series Aruba CX 4100i Switch Series Aruba CX 6000 Switch Series Aruba CX 6100 Switch Series Aruba CX 6200F Switch Series Aruba CX 6300 Switch Series Aruba CX 6400 Switch Series Aruba CX 8320 Switch Series Aruba CX 8325 Switch Series Aruba CX 8360 Switch Series Aruba CX 8400 Switch Series Aruba CX 9300 Switch Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04818en_us&docLocale=en_US

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39279, CVE-2024-28047)
Description	F5 has released security updates addressing Multiple Vulnerabilities that exist in their Product. **CVE-2024-39279 -** Insufficient granularity of access control in UEFI firmware in some Intel(R) processors may allow a authenticated user to potentially enable denial of service via local access. **CVE-2024-28047 -** Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A Versions - 1.8.0, 1.5.1 - 1.5.2 F5OS-C Versions - 1.8.0, 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000150432

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.