Advisory Alert

Alert Number: AAA20250320 **Date:** March 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Remote Code Execution Vulnerability
Dell	**High**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Oracle	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Cross Site Scripting Vulnerabilities
F5	**Medium**	Speculative Race Conditions Vulnerability
FortiGuard	**Medium**	Stack Buffer Overflow Vulnerability

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-23120)
Description	Veeam has released a security update addressing a vulnerability which affects Veeam Backup & Replication, allowing Remote Code Execution (RCE) by authenticated domain users. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.0.310 and all earlier version 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4724

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-22667)
Description	Dell has released security updates addressing a vulnerability that exists in a third party product which affects Dell ECS. **CVE-2024-22667** - Vim before 9.0.2142 has a stack-based buffer overflow because did_set_langmap in map.c calls sprintf to write to the error buffer that is passed down to the option callback functions. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell ECS versions prior to 3.8.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000296050/dsa-2025-092-security-update-for-dell-ecs-3-8-1-4-vulnerability

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-10176, CVE-2025-22150, CVE-2024-56374, CVE-2017-13693)
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in third party products which affects Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Solaris 11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/bulletinjan2025.html

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Cross Site Scripting Vulnerabilities
Description	Drupal has released security updates addressing multiple Cross Site Scripting Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Core versions: Drupal 8.0.0 and later up to but not including 10.3.14 Drupal 10.4.0 and later up to but not including 10.4.5 Drupal 11.0.0 and later up to but not including 11.0.13 Drupal 11.1.0 and later up to but not including 11.1.5 Formatter Suite module versions prior to 2.1.0 for Drupal 10 RapiDoc OAS Field Formatter module versions prior to 1.0.1 for Drupal 10 Link field display mode formatter module versions prior to 1.6.0 for Drupal 10 and 11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-core-2025-004 • https://www.drupal.org/sa-contrib-2025-026 • https://www.drupal.org/sa-contrib-2025-025 • https://www.drupal.org/sa-contrib-2025-024

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Speculative Race Conditions Vulnerability (CVE-2024-2193)
Description	F5 has released security updates addressing a Speculative Race Conditions Vulnerability that exists in F5OS, Traffix SDC and BIG-IP Next modules. **CVE-2024-2193** - A Speculative Race Condition (SRC) vulnerability that impacts modern CPU architectures supporting speculative execution (related to Spectre V1) has been disclosed. An unauthenticated attacker can exploit this vulnerability to disclose arbitrary data from the CPU using race conditions to access the speculative executable code paths. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) versions 20.0.1 - 20.1.0 BIG-IP Next Central Manager versions 20.0.1 - 20.2.0 F5OS-A versions 1.7.0, 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2 Traffix SDC 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139682

Affected Product	**FortiGuard**
Severity	**Medium**
Affected Vulnerability	Stack Buffer Overflow Vulnerability (CVE-2024-46663)
Description	FortiGuard has released security updates addressing a Stack Buffer Overflow Vulnerability that exists in CLI command which affect FortiMail. **CVE-2024-46663** - A stack-buffer overflow vulnerability in FortiMail CLI may allow a privileged attacker to execute arbitrary code or commands via specifically crafted CLI commands. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiMail 7.6 versions 7.6.0 through 7.6.1 FortiMail 7.4 versions 7.4.0 through 7.4.3 FortiMail 7.2 versions 7.2.0 through 7.2.6 FortiMail 7.0 all versions FortiMail 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-331

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.