Advisory Alert

Alert Number: AAA20241128 **Date:** November 28, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
ManageEngine	**High**	Sensitive Data Exposure Vulnerability
Synology	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Drupal	**Medium**	Cross Site Scripting Vulnerability
QNAP	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**ManageEngine**
Severity	**High**
Affected Vulnerability	Sensitive Data Exposure vulnerability (CVE-2024-52323)
Description	ManageEngine has released security updates addressing a Sensitive Data Exposure Vulnerability that exists in their products. **CVE-2024-52323 -** A Sensitive Data Exposure vulnerability has been identified in Analytics Plus, allowing an authenticated user to retrieve sensitive tokens associated to the org-admin account. This could potentially lead to unintended privilege escalation. ManageEngine advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ManageEngine Analytics Plus builds Prior to Build 6100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.manageengine.com/analytics-plus/CVE-2024-52323.html

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology 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, Obtain Sensitive Information, Users to Obtain Privileges Without Consent. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology DSM 7.2.2 Prior to 7.2.2-72806 Synology DSM 7.2.1 Prior to 7.2.1-69057-2 Synology DSMUC 3.1 Prior to 3.1.4-23079
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_27

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 cause Use-after-free, Buffer overflow, Race Condition, Memory Leak. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Micro 5.1 to 5.4 SUSE Linux Enterprise Micro for Rancher 5.2 to 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244081-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244082-1/

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross Site Scripting Vulnerability
Description	Drupal has released security updates addressing a Cross Site Scripting Vulnerability that exists 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	Tarte au citron Module Versions Prior to 2.0.5 for Drupal 10.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-064

Affected Product	**QNAP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-32771, CVE-2023-39298, CVE-2024-53691)
Description	QNAP has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2024-32771 -** The improper restriction of excessive authentication attempts vulnerability could allow attackers to use brute force attacks to gain privileged access. **CVE-2023-39298 -** The missing authorization vulnerability could allow local attackers who have gained user access to access data or perform actions without the proper privileges. **CVE-2024-53691 -** The link following vulnerability could allow remote attackers who have gained user access to traverse the file system to unintended locations. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QNAP QTS 5.1.x QNAP QuTS hero h5.1.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-28

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-32573)
Description	F5 has released security updates addressing a Denial of Service Vulnerability that exists in their products. CVE-2023-32573 - In Qt before 5.15.14, 6.0.x through 6.2.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1, QtSvg QSvgFont m_unitsPerEm initialization is mishandled. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP 17.x 17.1.0 - 17.1.1 BIG-IP 16.x 16.1.0 - 16.1.5 BIG-IP 15.x 15.1.0 - 15.1.10 Traffix SDC 5.x 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148690

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.