Advisory Alert

Alert Number: AAA20240606 **Date:** June 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
F5	**Low**	Arbitrary Code Execution Vulnerability

Description

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in acquia_dam module. Flaw in Acquia DAM that doesn't sufficiently protect the ability to disconnect a site from DAM. While disconnected sites do not lose asset data in Drupal, it will prevent site editors from accessing the DAM until a site administrator re-authenticates the site. Some uncached media images may also fail to be fetched while disconnected. This flaw can lead to Access Bypass and Denial of Service vulnerabilities in Drupal. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	acquia_dam module versions below 1.0.13 for Drupal 9.4 or above pre-release versions of acquia_dam 1.1.0 before version 1.1.0-beta3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-025

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20404, CVE-2024-20405)
Description	Cisco has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2024-20404** - A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. **CVE-2024-20405** - A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Finesse Release 11.6(1) ES11 and earlier Cisco Finesse Release 12.6(2) ES01 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-25162, CVE-2020-36777, CVE-2021-46934, CVE-2021-47013, CVE-2021-47055, CVE-2021-47118, CVE-2021-47153, CVE-2021-47171, CVE-2021-47185, CVE-2022-48627, CVE-2023-6240, CVE-2023-52439, CVE-2023-52445, CVE-2023-52477, CVE-2023-52513, CVE-2023-52520, CVE-2023-52528, CVE-2023-52565, CVE-2023-52578, CVE-2023-52594, CVE-2023-52595, CVE-2023-52610, CVE-2024-0340, CVE-2024-23307, CVE-2024-25744, CVE-2024-26593, CVE-2024-26603, CVE-2024-26610, CVE-2024-26615, CVE-2024-26642, CVE-2024-26643, CVE-2024-26659, CVE-2024-26664, CVE-2024-26693, CVE-2024-26694, CVE-2024-26743, CVE-2024-26744, CVE-2024-26779, CVE-2024-26872, CVE-2024-26892, CVE-2024-26897, CVE-2024-26901, CVE-2024-26919, CVE-2024-26933, CVE-2024-26934, CVE-2024-26964, CVE-2024-26973, CVE-2024-26993, CVE-2024-27014, CVE-2024-27048, CVE-2024-27052, CVE-2024-27056, CVE-2024-27059)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information disclosure, Integer overflow, Memory corruption, Use-after-free conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:3627

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2017-18342)
Description	F5 has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in their products. **CVE-2017-18342** - Vulnerbility In PyYAML before 5.1, the yaml.load() API could execute arbitrary code if used with untrusted data. The load() function has been deprecated in version 5.1 and the 'UnsafeLoader' has been introduced for backward compatibility with the function. 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 - 16.1.4 BIG-IP (all modules) 15.x versions 15.1.0 - 15.1.10 BIG-IQ Centralized Management 8.x 8.1.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139901

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.