Advisory Alert

Alert Number: AAA20220527 **Date:** May 27, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Cookie Middleware Vulnerability
Dell	**High**	Multiple Vulnerabilities
Redhat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Cookie Middleware Vulnerability (CVE-2022-29248)
Description	Durpal has released a workaround/patch for a vulnerability that exists in Guzzle (which is a PHP HTTP client) prior to versions 6.5.6 and 7.4.3 with the cookie middleware. The vulnerability is that it is not checked if the cookie domain equals the domain of the server which sets the cookie via the Set-Cookie header, allowing a malicious server to set cookies for unrelated domains. The cookie middleware is disabled by default, and most library consumers will not be affected by this issue. It affects only those who manually add the cookie middleware to the handler stack or construct the client with ['cookies' => true]. Moreover, those who do not use the same Guzzle client to call multiple domains and have disabled redirect forwarding are not affected by this vulnerability. Guzzle versions 6.5.6 and 7.4.3 contain a patch for this issue. As a workaround, turn off the cookie middleware.
Affected Products	Drupal 9.3 Drupal 9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-010

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2015-8985, CVE-2018-20573, CVE-2018-20574, CVE-2018-25032, CVE-2019-6285, CVE-2019-6292, CVE-2021-0920, CVE-2021-22570, CVE-2021-25220, CVE-2021-31799, CVE-2021-31810, CVE-2021-32066, CVE-2021-3778, CVE-2021-3796, CVE-2021-3872, CVE-2021-3927, CVE-2021-3928, CVE-2021-39698, E-2021-3984, CVE-2021-3999, CVE-2021-4019, CVE-2021-41617, CVE-2021-41817, CVE-2021-4193, CVE-2021-44879, CVE-2021-45868, CVE-2021-46059, CVE-2022-0001, CVE-2022-0002, CVE-2022-0318, CVE-2022-0319, CVE-2022-0351, CVE-2022-0361, CVE-2022-0413, CVE-2022-0435, CVE-2022-0487, CVE-2022-0492, CVE-2022-0516, CVE-2022-0617, CVE-2022-0644, CVE-2022-0778, CVE-2022-0847, CVE-2022-0850, CVE-2022-0854, CVE-2022-0934, CVE-2022-1015, CVE-2022-1016, CVE-2022-1048, CVE-2022-1055, CVE-2022-1097, CVE-2022-1271, CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21476, CVE-2022-21496, CVE-2022-22934, CVE-2022-22935, CVE-2022-22936, CVE-2022-22941, CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042, CVE-2022-23181, CVE-2022-23218, CVE-2022-23219, CVE-2022-24407, CVE-2022-24448, CVE-2022-24958, CVE-2022-24959, CVE-2022-25235, CVE-2022-25236, CVE-2022-25258, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315, CVE-2022-25375, CVE-2022-26490, CVE-2022-26966, CVE-2022-27666, CVE-2022-28388, CVE-2022-28389, CVE-2022-28390, CVE-2022-28739)
Description	Dell has released remediation addressing multiple vulnerabilities that exists in their products that may be exploited by malicious users to compromise the affected system. It is recommended by DELL to take necessary remediation steps to avoid issues.
Affected Products	Dell VxRail7.0.x versions before 7.0.371
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000200092/dsa-2022-136-dell-vxrail-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3807, CVE-2021-23425, CVE-2021-33502, CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2022-24302, CVE-2022-0207)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause denial of service, cross site scripting attacks, disclosure of sensitive values in log files and unauthorized information disclosure. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Virtualization for IBM Power LE 4 for RHEL 8 ppc64le Red Hat Virtualization Manager 4.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:4711 https://access.redhat.com/errata/RHSA-2022:4712 https://access.redhat.com/errata/RHSA-2022:4764

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.