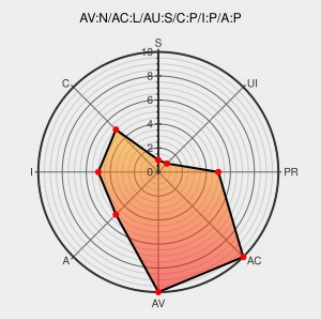
CVE-2015-1561

Published on: 07/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1561

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Centreon from Centreon contain the following vulnerability:

The escape_command function in include/Administration/corePerformance/getStats.php in Centreon (formerly Merethis Centreon) 2.5.4 and earlier (fixed in Centreon 19.10.0) uses an incorrect regular expression, which allows remote authenticated users to execute arbitrary commands via shell metacharacters in the ns_id parameter.

CVE-2015-1561 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20150708 Merethis Centreon - Unauthenticated blind SQLi and Au Command Execution
enh(secu): removing unused file · centreon/centreon@a78c60a · GitHub	github.com text/html	MISC github.com/centreon/centreon/commit/a78c60aad6fd5af9b51a6d5de5d6 27550b563fa8d660b64bca871a219cb1
403 Forbidden	forge.centreon.com text/html Inactive Link Not Archived	CONFIRM forge.centreon.com/projects/centreon/repository/revisions/387dffdd051dbc7a234e
Merethis Centreon 2.5.4 SQL Injection / Remote	Exploit packetstormsecurity.com	MISC packetstormsecurity.com/files/132607/Merethis-Centreon-2.5.4-SQL-Inje Command-Execution.html

Command Execution ≈ Packet Storm

text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

994844 PHP (Composer) Security Update for centreon/centreon (GHSA-c4fj-3wqq-g9c9)

Exploit/POC from Github

A little Python tool for exploiting CVE-2015-1560 and CVE-2015-1561. Quick'n'dirty. Real dirty.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Centreon	Centreon	All	All	All	All

cpe:2.3:a:centreon:centreon:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→