



# CVE-2018-21025

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-21025
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-08 13:15:00 UTC
<b>Updated</b>	2019-10-11 15:57:00 UTC
<b>Description</b>	In Centreon VM through 19.04.3, centreon-backup.pl allows attackers to become root via a crafted script, due to incorrect ri

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
oss-security - Multiple vulnerabilities in Centreon-Web and Centreon-VM	MISC	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third
oss-security - Re: Multiple vulnerabilities in Centreon-Web and Centreon-VM	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third
[security] Privilege Escalation from crontab · Issue #7082 · centreon/centreon · GitHub	MISC	<a href="https://github.com">github.com</a>	Exploit, Third Par
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)