



# CVE-2020-14424

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

## Summary

<b>CVE</b>	CVE-2020-14424
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-14 20:15:00 UTC
<b>Updated</b>	2021-11-16 18:49:00 UTC
<b>Description</b>	Cacti before 1.2.18 allows remote attackers to trigger XSS via template import for the midwinter theme.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

## References

### Reference

Lack of escaping on template import can lead to XSS exposure under 'midwinter' theme (CVE-2020-14424) by ddb4github · Pull Request #426

2001016 – (CVE-2020-14424) CVE-2020-14424 cacti: lack of escaping on template import can lead to XSS

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[282049](#) Fedora Security Update for cacti (FEDORA-2021-818ff2c12b)

[282050](#) Fedora Security Update for cacti (FEDORA-2021-cfc1913b5f)

[751044](#) OpenSUSE Security Update for cacti, cacti-spine (openSUSE-SU-2021:1190-1)

[751045](#) OpenSUSE Security Update for cacti, cacti-spine (openSUSE-SU-2021:1190-1)

---

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**