



# CVE-2020-7237

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

## Summary

<b>CVE</b>	CVE-2020-7237
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-20 05:15:00 UTC
<b>Updated</b>	2023-11-07 03:25:00 UTC
<b>Description</b>	Cacti 1.2.8 allows Remote Code Execution (by privileged users) via shell metacharacters in the Performance Boost Debug

## Risk And Classification

### Problem Types: CWE-78

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cacti</a>	<a href="#">Cacti</a>	1.2.8	All	All	All
Application	<a href="#">Cacti</a>	<a href="#">Cacti</a>	1.2.8	All	All	All

## References

### Reference

[security-announce] openSUSE-SU-2020:0284-1: important: Security update
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists
[CVE-2020-7237] Remote Code Execution in Cacti RRDTOol – Chi Tran
[security-announce] openSUSE-SU-2020:0565-1: important: Security update
[security-announce] openSUSE-SU-2020:0558-1: important: Security update
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists
Cacti: Multiple vulnerabilities (GLSA 202003-40) — Gentoo security
Remote Code Execution due to input validation failure in Performance Boost Debug Log (CVE-2020-7237) · Issue #3201 · Cacti/cacti · GitHub
[security-announce] openSUSE-SU-2020:0272-1: important: Security update
CVE Program record

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500842](#) Alpine Linux Security Update for cacti

[504596](#) Alpine Linux Security Update for cacti

© [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](#)