



# CVE-2020-8813

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-8813
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-22 02:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	graph_realtime.php in Cacti 1.2.8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in a

## 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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Suse Linux Enterprise Server</a>	12.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Suse Package Hub</a>	All	All	All	All
Application	<a href="#">Opmantek</a>	<a href="#">Open-audit</a>	3.3.1	All	All	All

## References

Reference	S
Cacti v1.2.8 authenticated Remote Code Execution (CVE-2020-8813) - Shells.Systems	M
[SECURITY] Fedora 31 Update: cacti-1.2.10-1.fc31 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 30 Update: cacti-spine-1.2.10-1.fc30 - package-announce - Fedora Mailing-Lists	F
Releases · Cacti/cacti · GitHub	M
[SECURITY] Fedora 32 Update: cacti-1.2.10-1.fc32 - package-announce - Fedora Mailing-Lists	F

CactiExploit-2020-02-08_05.46.38.mp4 - Google Drive	M
Open-Audit Professional 3.3.1 Remote Code Execution ≈ Packet Storm	M
When guest users have access to realtime graphs, remote code could be executed (CVE-2020-8813) · Issue #3285 · Cacti/cacti · GitHub	C
Cacti 1.2.8 Unauthenticated Remote Code Execution ≈ Packet Storm	M
[SECURITY] Fedora 31 Update: cacti-1.2.10-1.fc31 - package-announce - Fedora Mailing-Lists	F
[SECURITY] Fedora 32 Update: cacti-1.2.10-1.fc32 - package-announce - Fedora Mailing-Lists	
[security-announce] openSUSE-SU-2020:0565-1: important: Security update	S
[security-announce] openSUSE-SU-2020:0558-1: important: Security update	S
Cacti 1.2.8 Authenticated Remote Code Execution ≈ Packet Storm	M
[SECURITY] Fedora 30 Update: cacti-spine-1.2.10-1.fc30 - package-announce - Fedora Mailing-Lists	
cacti-exploit.py · GitHub	M
[SECURITY] [DLA 3252-1] cacti security update	M
Cacti 1.2.8 Unauthenticated Remote Code Execution ≈ Packet Storm	M
Cacti: Multiple vulnerabilities (GLSA 202004-16) — Gentoo security	G
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[181453](#) Debian Security Update for cacti (DLA 3252-1)

[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](#)