



# CVE-2020-7106

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

## Summary

<b>CVE</b>	CVE-2020-7106
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-16 04:15:00 UTC
<b>Updated</b>	2023-11-07 03:25:00 UTC
<b>Description</b>	Cacti 1.2.8 has stored XSS in data_sources.php, color_templates_item.php, graphs.php, graph_items.php, lib/api_automati

## 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
Application	Cacti	Cacti	1.2.8	All	All	All
Application	Cacti	Cacti	1.2.8	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Application	Fedoraproject	Extra Packages For Enterprise Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Suse	Linux Enterprise	12.0	All	All	All
Application	Suse	Package Hub	-	All	All	All

## References

Reference	Source	Link
-----------	--------	------

[security-announce] openSUSE-SU-2020:0284-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2020:0654-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>
[SECURITY] [DLA 2965-1] cacti security update	MLIST	<a href="#">lists.debian.org</a>
[security-announce] openSUSE-SU-2020:0565-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2020:0558-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Lack of escaping on some pages can lead to XSS exposure (CVE-2020-7106) · Issue #3191 · Cacti/cacti · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] [DLA 2069-1] cacti security update	MLIST	<a href="#">lists.debian.org</a>
Cacti: Multiple vulnerabilities (GLSA 202003-40) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[security-announce] openSUSE-SU-2020:0272-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[179164](#) Debian Security Update for cacti (DLA 2965-1)

[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](#)