



Security

Get Gentoo!

[gentoo.org sites](https://gentoo.org/sites)

[gentoo.org Wiki](https://gentoo.org/wiki) [Bugs](#) [Forums](#) [Packages](#)

[Planet](#) [Archives](#) [Sources](#)

[Infra Status](#)

□

- [Home](#)
- [Stay informed](#)
- [Advisories](#)

Cacti: Multiple vulnerabilities — GLSA 202007-03

Multiple vulnerabilities have been found in Cacti, the worst of which could result in the arbitrary execution of code.

Affected packages

Package net-analyzer/cacti on all architectures

Affected versions < 1.2.13

Unaffected versions >= 1.2.13

Package net-analyzer/cacti-spine on all architectures

Affected versions < 1.2.13

Unaffected versions >= 1.2.13

Background

Cacti is a complete frontend to rrdtool.

Description

Multiple vulnerabilities have been discovered in Cacti. Please review the CVE identifiers referenced below for details.

Impact

Please review the referenced CVE identifiers for details.

Workaround

There is no known workaround at this time.

Resolution

All Cacti users should upgrade to the latest version:

```
# emerge --sync  
# emerge --ask --oneshot --verbose ">=net-analyzer/cacti-1.2.13"
```

All Cacti Spine users should upgrade to the latest version:

```
# emerge --sync  
# emerge --ask --oneshot --verbose ">=net-analyzer/cacti-spine-1.2.13"
```

References

- [CVE-2020-11022](#)
- [CVE-2020-11023](#)
- [CVE-2020-14295](#)

Release date

July 26, 2020

Latest revision

July 26, 2020: 1

Severity

normal

Exploitable

remote

Bugzilla entries

- [728678](#)
- [732522](#)

Questions or comments?

Please feel free to [contact us](#).

-
-

© 2001–2026 Gentoo Foundation, Inc.

Gentoo is a trademark of the Gentoo Foundation, Inc. The contents of this document, unless otherwise expressly stated, are licensed under the [CC-BY-SA-4.0](#) license. The [Gentoo name and logo usage guidelines](#) apply.