



Security

[Get Gentoo!](#)

[gentoo.org sites](#)

[gentoo.org Wiki](#) [Bugs](#) [Forums](#) [Packages](#)

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

[Infra Status](#)

□

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

cURL: Multiple vulnerabilities — GLSA 202003-29

Multiple vulnerabilities have been found in cURL, the worst of which may lead to arbitrary code execution.

Affected packages

Package `net-misc/curl` on all architectures

Affected versions `< 7.66.0`

Unaffected versions `>= 7.66.0`

Background

A command line tool and library for transferring data with URLs.

Description

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

Impact

A remote attacker could possibly execute arbitrary code with the privileges of the process or cause a Denial of Service condition.

Workaround

There is no known workaround at this time.

Resolution

All cURL users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-misc/curl-7.66.0"
```

References

- [CVE-2019-5435](#)
- [CVE-2019-5436](#)
- [CVE-2019-5481](#)
- [CVE-2019-5482](#)

Release date

March 15, 2020

Latest revision

March 15, 2020: 1

Severity

normal

Exploitable

remote

Bugzilla entries

- [686050](#)
- [694020](#)

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.