



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 201709-14

Multiple vulnerabilities have been found in cURL, the worst of which may allow attackers to bypass intended restrictions.

### Affected packages

**Package** `net-misc/curl` on all architectures

**Affected versions** `< 7.55.1`

**Unaffected versions** `>= 7.55.1`

### Background

cURL is a tool and libcurl is a library for transferring data with URL syntax.

### Description

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

### Impact

Remote attackers could cause a Denial of Service condition, obtain sensitive information, or bypass intended restrictions for TLS sessions.

### 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-7.55.1"
```

## References

- [CVE-2017-1000099](#)
- [CVE-2017-1000100](#)
- [CVE-2017-1000101](#)
- [CVE-2017-7407](#)
- [CVE-2017-7468](#)

### Release date

September 17, 2017

### Latest revision

September 17, 2017: 1

### Severity

normal

### Exploitable

remote

### Bugzilla entries

- [615870](#)
- [615994](#)
- [626776](#)

## 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.