



\_Security

### [Get Gentoo!](#)

[gentoo.org sites](#)

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

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

[Infra Status](#)

□

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

# OpenSSL: Multiple Vulnerabilities — GLSA 202211-01

Multiple vulnerabilities have been discovered in OpenSSL, the worst of which could result in remote code execution.

## Affected packages

**Package** `dev-libs/openssl` on all architectures

**Affected versions** `< 3.0.7`

**Unaffected versions** `>= 3.0.7`

## Background

OpenSSL is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) as well as a general purpose cryptography library.

## Description

Multiple buffer overflows exist in OpenSSL's handling of TLS certificates for client authentication.

## Impact

It is believed that, while unlikely, code execution is possible in certain system configurations.

## Workaround

Users operating TLS servers may consider disabling TLS client authentication, if it is being used, until fixes are applied.

## Resolution

All OpenSSL 3 users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=dev-libs/openssl-3.0.7"
```

## References

- [CVE-2022-3602](#)
- [CVE-2022-3786](#)

### Release date

November 01, 2022

### Latest revision

November 01, 2022: 1

### Severity

normal

### Exploitable

remote

### Bugzilla entries

- [878269](#)

## 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.