OpenSSL: Multiple Vulnerabilities — GLSA 202210-02

Multiple vulnerabilities have been discovered in OpenSSL, the worst of which could result in denial of service.

Affected packages

Package	**dev-libs/openssl** on all architectures
Affected versions	< **1.1.1q**
Unaffected versions	>= **1.1.1q**

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 vulnerabilities have been discovered in OpenSSL. 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 OpenSSL users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=dev-libs/openssl-1.1.1q"
```

References

- CVE-2020-1968
- CVE-2021-3711
- CVE-2021-3712
- CVE-2021-4160
- CVE-2022-0778
- CVE-2022-1292
- CVE-2022-1473
- CVE-2022-2097

Release date
October 16, 2022

Latest revision
October 16, 2022: 1

Severity
normal

Exploitable
remote

Bugzilla entries

- 741570
- 809980
- 832339
- 835343
- 842489
- 856592

Questions or comments?

Please feel free to contact us.