OpenBSD 7.8 Errata

For errata on a certain release, click below:
2.0, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9.

Patches for the OpenBSD base system are distributed as unified diffs. Each patch is cryptographically signed with the signify(1) tool and contains usage instructions. All the following patches are also available in one tar.gz file for convenience.

Alternatively, the syspatch(8) utility can be used to apply binary updates. Full binary updates are made available on the following architectures: amd64, i386, arm64. On other architectures, only machine-independent updates are produced (and these are exceedingly rare).

Patches for supported releases are also incorporated into the -stable branch, which is maintained for one year after release.

- **001: RELIABILITY FIX: October 26, 2025** *All architectures*
  syspatch(8) is confused by aliased /dev/*rootdisk nodes in the database generated by dev_mkdb(8).
  A source code patch exists which remedies this problem.
  If syspatch fails (probably because /usr is not a separate filesystem), perform these steps:

```
sed -e 's/.checkfs/#checkfs/g' /usr/sbin/syspatch > /root/syspatch
ksh /root/syspatch
syspatch # re-run new syspatch command as instructed
rm /root/syspatch
dev_mkdb
```

- **002: SECURITY FIX: October 28, 2025** *All architectures*
  Use-after-free and integer overflow in the Xkb and Present X server extensions. CVE-2025-62229 CVE-2025-62230 CVE-2025-62231
  A source code patch exists which remedies this problem.

- **003: SECURITY FIX: October 28, 2025** *All architectures*
  DNS cache poisoning vulnerabilities in unbound could lead to domain hijacking. CVE-2025-11411
  A source code patch exists which remedies this problem.

- **004: RELIABILITY FIX: October 28, 2025** *All architectures*
  Ensure the group selected by a TLSv1.3 server for a HelloRetryRequest is not one for which the client has already sent a key share.
  A source code patch exists which remedies this problem.

- **005: SECURITY FIX: October 31, 2025** *All architectures*
  smtpd(8) can die if a malformed imsg is sent on the local socket. CVE-2025-62875
  A source code patch exists which remedies this problem.

- **006: RELIABILITY FIX: November 17, 2025** *All architectures*
  Missing modifications to libunwind after the LLVM 19.1.7 update can cause performance regressions and missing endbr instructions.
  A source code patch exists which remedies this problem.

- **007: RELIABILITY FIX: December 3, 2025** *All architectures*
  Fix drm(4) to avoid spurious sleep errors leading to crashes.
  A source code patch exists which remedies this problem.

- **008: SECURITY FIX: December 3, 2025** *All architectures*
  Fix buffer overflow vulnerabilities in libpng which is part of libfreetype. CVE-2025-64505 CVE-2025-64506 CVE-2025-64720 CVE-2025-65018
  A source code patch exists which remedies this problem.

- **009: SECURITY FIX: December 3, 2025** *All architectures*
  Fix incorrect handling of invalid inputs to xkbcomp(1). CVE-2018-15853 CVE-2018-15859 CVE-2018-15861 CVE-2018-15863
  A source code patch exists which remedies this problem.

- **010: SECURITY FIX: December 3, 2025** *All architectures*
  Fix incomplete mitigation of DNS cache poisoning vulnerabilities in unbound. CVE-2025-11411
  A source code patch exists which remedies this problem.

- **011: RELIABILITY FIX: December 3, 2025** *All architectures*
  Due to a race, the kernel could crash when adding IPv6 neighbor discovery entries.
  A source code patch exists which remedies this problem.

- **012: RELIABILITY FIX: January 14, 2026** *All architectures*
  A malicious RPKI Certification Authority can cause a NULL dereference. A malicious RPKI Trust Anchor can cause memory exhaustion.
  A source code patch exists which remedies this problem.

- **013: SECURITY FIX: February 2, 2026** *All architectures*
  Fix a use-after-free in httpd(8) when using chunked encoding.
  A source code patch exists which remedies this problem.

- **014: SECURITY FIX: February 9, 2026** *All architectures*
  In libexpat fix denial of service due to NULL dereference and integer overflow. CVE-2026-24515 CVE-2026-25210
  A source code patch exists which remedies this problem.

- **015: SECURITY FIX: February 27, 2026** *All architectures*
  Stop userland from using pledge(2) "tmppath" because the kernel feature will be removed soon.
  A source code patch exists which remedies this problem.

- **016: SECURITY FIX: February 27, 2026** *All architectures*
  sysctl requests blocked by pledge(2) create a diagnostic message which races inside pty(4) and possibly crashes.
  A source code patch exists which remedies this problem.

- **017: SECURITY FIX: March 2, 2026** *All architectures*
  In ldconfig(8), stop userland from using pledge(2) "tmppath" because the kernel feature will be removed soon.
  A source code patch exists which remedies this problem.

- **018: SECURITY FIX: March 4, 2026** *All architectures*
  Make the pledge(2) mechanism which permits specific libc paths more strict by removing the "tmppath" promise, avoid normalizing paths which libc already creates strictly correct, and blocking '..' traversals out of /usr/share/zoneinfo.
  A source code patch exists which remedies this problem.

Ports that use pledge "tmppath" have to be adapted and rebuilt before rebooting.
Affected are:
- devel/got,-server
- graphics/arcan
- mail/opensmtpd-filters/dkimsign
- math/moo
- net/gmid
- net/iperf3
- security/pizauth
- security/ruby-pledge,ruby33
- sysutils/fzf
- sysutils/rset
- www/chromium
- www/firefox-esr
- www/iridium
- www/mozilla-firefox
- www/tor-browser/browser
- www/ungoogled-chromium

With OpenBSD 7.8 on the amd64 and i386 architecture, you can update stable packages.

- **019: SECURITY FIX: March 4, 2026** *All architectures*
unveil(2) traversals could misbehave crossing mountpoints.
A source code patch exists which remedies this problem.

- **020: SECURITY FIX: March 10, 2026** *All architectures*
Prevent an integer overflow leading to out-of-bounds read in FreeType. CVE-2026-23865
A source code patch exists which remedies this problem.

- **021: RELIABILITY FIX: March 10, 2026** *All architectures*
Stop userland from using pledge(2) "tmppath" because the kernel feature has been removed.
The calendar binary was missing from previous syspatch.

- **022: SECURITY FIX: March 15, 2026** *All architectures*
pledge(2) "recvfd" should not kill a process who receives bad descriptors.
A source code patch exists which remedies this problem.

- **023: RELIABILITY FIX: March 19, 2026** *All architectures*
calendar(1) could not send mail due to missing unveil.
A source code patch exists which remedies this problem.

- **024: RELIABILITY FIX: March 21, 2026** *All architectures*
In libexpat fix denial of service due to NULL dereference and infinite loop. CVE-2026-32776 CVE-2026-32777 CVE-2026-32778
A source code patch exists which remedies this problem.

- **025: RELIABILITY FIX: March 25, 2026** *All architectures*
TCP packets with invalid SACK options could crash the kernel.
A source code patch exists which remedies this problem.

- **026: RELIABILITY FIX: March 27, 2026** *All architectures*
In smtpd(8), an LF character in the username or password could stop proc tables, causing a denial of service.
A source code patch exists which remedies this problem.

- **027: SECURITY FIX: April 4, 2026** *All architectures*
In iked(8) add stricter checks to avoid out-of-bounds read, NULL pointer dereference, and keep the state

machine consistent.
A source code patch exists which remedies this problem.

- **028: SECURITY FIX: April 14, 2026** *All architectures*
  Multiple vulnerabilites in the X server sync and Xkb extensions. CVE-2026-33999 CVE-2026-34000 CVE-2026-34001 CVE-2026-34002 CVE-2026-34003
  A source code patch exists which remedies this problem.

- **029: RELIABILITY FIX: April 14, 2026** *All architectures*
  rad(8) and slaacd(8) could spin doing nothing after a malformed packet.
  A source code patch exists which remedies this problem.

- **030: RELIABILITY FIX: April 14, 2026** *All architectures*
  A malicious RPKI Publication Server can cause an incorrect error exit. A malicious RRDP Publication Server can cause a NULL dereference.
  A source code patch exists which remedies this problem.

- **031: SECURITY FIX: April 17, 2026** *All architectures*
  pgrp management through a fork is unsafe.
  A source code patch exists which remedies this problem.
