



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next>] [day] [month] [year] [list]

Message-ID: <20260430182126.GA28748@openwall.com>
 Date: Thu, 30 Apr 2026 20:21:26 +0200
 From: Solar Designer <solar@...nwall.com>
 To: oss-security@...ts.openwall.com
 Cc: Bernard Quatermass <bernardq@...m.org>, security@...m.org
 Subject: Exim 4.99.2 fixes 4 CVEs

Bernard helpfully notified distros of this upcoming security release on April 24 and then of the release itself on April 29, but unfortunately did not bring this to oss-security as expected - so I am doing it now, delayed by one day.

This was also sent to the public exim-announce list yesterday:

<https://lists.exim.org/lurker/message/20260429.121733.f58d9686.en.html>

but it isn't prominently visible on the Exim website now. I tried clicking the Security link in the navigation on top, but this merely opened a directory listing with some text files and subdirectories in there, with all file timestamps showing as 30-Apr-2026 10:29 and so nothing clearly standing out as new. Looks like something to improve.

----- Forwarded message from Bernard Quatermass <bernardq@...m.org> -----

From: Bernard Quatermass <bernardq@...m.org>
 To: "Distros @ oss-security openwall" <distros@...openwall.org>
 Subject: Re: [vs-plain] EXIM-Security-2026-04-24
 CC: "security@...m.org" <security@...m.org>
 Date: Wed, 29 Apr 2026 13:19:42 +0100

we are pleased to announce the availability of release 4.99.2 of Exim.

This is a security release.

It fixes the following vulnerabilities.

CVE-2026-40684 Possible crash with malicious DNS data when using musl libc

On systems using musl libc (not glibc) due to an oddity in octal printing it is possible to crash the connection instance when malformed DNS data is present in PTR records.

CVE-2026-40685 Possible OOB read/write on corrupt JSON in header

configurations using json operators on invalid externally-provided input could trigger heap corruption.

CVE-2026-40686 Possible OOB read with large UTF8 trailing characters

configurations using utf8 operators on malformed utf8 in headers could trigger OOB reads and might trigger some data leak if error messages are required for subsequent emails in the current connection and similar malformed headers are present.

CVE-2026-40687 Possible OOB read/write with SPA authenticator

in configurations using the SPA authentication driver to a hostile/compromised external SPA/NTLM connection it is possible to trigger an OOB read/write and crash the connection instance or possibly leak heap data to the instance.

Older Exim versions may or may not be vulnerable but are not actively maintained.

We would like to thank the thousands of unnamed and uncredited authors whose works were ingested into the slopbots to "assist" in the reports for these vulnerabilities.

Exim 4.99.2 is available:

- * as tarball
- * <https://ftp.exim.org/pub/exim/exim4/>
- * <https://code.exim.org/exim/exim/releases>

- * directly from Git: <https://code.exim.org/exim/exim>
tag: exim-4.99.2

The signatures on the release tarballs should be

- * key ID 0xBCE58C8CE41F32DF
Email: jgh@...m.org

--
Bernard Quatermass

----- End forwarded message -----

[Powered by blists - more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).