Skip to site navigation (Press enter)

[pfx-ann] Postfix stable release 3.11.2 and legacy releases 3.10.9, 3.9.10, 3.8.16

Wietse Venema via Postfix-announce Sun, 03 May 2026 16:49:08 -0700

[An on-line version of this announcement will be available at
https://www.postfix.org/announcements/postfix-3.11.2.html]

Fixed in Postfix 3.11:

  * Bugfix (defect introduced: Postfix 3.11): the proxymap(8) daemon
    dereferenced an uninitialized pointer after a request protocol
    error. This daemon is not exposed to local or remote users.
    Found by Claude Opus 4.6.

  * Bugfix (defect introduced: 20260309) a change, to set the
    service_name default value to "amnesiac", violated a test that
    parameter names in postconf output must match 1:1 with parameter
    names in the postlink script.

Fixed in Postfix 3.10:

  * Bugfix (defect introduced: Postfix 3.10): The RFC 2047 encoder
    for the sender "full name" could loop when a very long
    full_name_encoding_charset value was configured in main.cf.
    Found by Claude Opus 4.6.

Fixed in Postfix 3.8, 3.9, 3.10:

  * Bugfix (defect introduced: Postfix 2.3, date: 20050323): buffer
    over-read when Postfix an enhanced status code is not followed
    by other text. For example, "5.7.2" without text after the
    three-number code. This CANNOT be triggered with an SMTP or
    LMTP server response; is confirmed with an access(5) table and
    likely with a policy server response; can possibly be triggered
    with pipe-to-command output, header_checks(5), body_checks(5),
    an error(8) transport in transport_maps, or a milter response;
    and is confirmed with a DNSBL server TXT response while Postfix
    is configured with "$rbl_code $rbl_text" in rbl_reply_maps or
    default_rbl_reply. This could result in process termination.
    Problem reported by Kamil Frankowicz.

  * For older Postfix versions, a buffer over-read patch is included
    at the end of this text.

  * Code cleanup: log a fatal error instead of dereferencing a null
    pointer after a first/next cursor initialization failure. Fedor
    Vorobev. This affected the Berkeley DB client.

Fixed in Postfix 3.8, 3.9, 3.10. 3.11:

  * Portability: support for recent FreeBSD, NetBSD, and OpenBSD
    versions. Brad Smith.

  * Bugfix (defect introduced: Postfix 2.2, date 20041207): When
    truncating a database file, the cdb: database client looked at
    the file size from before requesting an exclusive lock on a

```
     database file, instead of the file size after the exclusive
     lock was granted. Found by Claude Opus 4.6.

   * Bugfix (defect introduced: Postfix alpha, date 19980309): file
     descriptor leak after fork() failure. Found by Claude Opus 4.6.

   * Mistakes in debug logging. Found by Claude Opus 4.6. This
     affected two files in Postfix 3.8 and 3.9, three files in Postfix
     3.10 and 3.11.

   * Unchecked null pointer results after an out-of-memory condition
     in a library dependency. Found by Claude Opus 4.6. The fix is
     to return an error status or to log a fatal error. This affected
     three source files.

   * Missing or incomplete guards for ssize_t or int overflow, found
     by Claude Opus 4.6. This affected three source files. These
     limits are unlikely to be exceeded because the size of in-memory
     objects is limited by design (the number of in-memory objects
     is also limited).

You can find the updated Postfix source code at the mirrors listed
at https://www.postfix.org/.

        Wietse

Buffer over-read patch for Postfix 2.3 .. 3.7:

--- /var/tmp/postfix-3.8.15/src/global/dsn_util.c       2006-01-07
20:28:37.000000000 -0500
+++ src/global/dsn_util.c       2026-05-01 16:59:50.961688175 -0400
@@ -155,5 +155,5 @@
        strncpy(dp->dsn.data, cp, len);
        dp->dsn.data[len] = 0;
-       cp += len + 1;
+       cp += len;
     } else if ((len = dsn_valid(def_dsn)) > 0) {
        strncpy(dp->dsn.data, def_dsn, len);
_______________________________________________
Postfix-announce mailing list -- postfix-announce@postfix.org
To unsubscribe send an email to postfix-announce-le...@postfix.org
```


- Previous message
- View by thread
- View by date
- Next message

Reply via email to