repos / mail-hardening

```
git clone https://coredump.ws/repos/mail-hardening.git
# push (client certificate):
git remote set-url --push origin https://coredump.ws:8443/repos/mail-hardening.git
```

Branches and tags

master	branch	16 days ago	**zip**

Files at HEAD (6a311bcd6b) · **download zip**

config/	
overlay/	
upstream/	
LICENSE	34.3 KB
README.md	30.8 KB

Recent commits · **all**

6a311bcd	Relicense under GPL-3.0-or-later	no-body-in-particular	16 days ago
3ccf5ce4	License under GPL-2.0	no-body-in-particular	16 days ago
44e94574	monitoring: mail-autofile files abuse-report traffic and system reports into an Automated folder	no-body-in-particular	18 days ago
b36e0a68	r7: re-inject scanned mail over a milter-less 127.0.0.1:10026 smtpd; sign local+remote mail	no-body-in-particular	19 days ago
3e894d98	upstream/opendkim-develop: OpenDKIM fixes ported to develop f6572323, with reproducer	coredump.ws	19 days ago
787ce8d5	dovecot 2.4.5-r4: 0030-0036 (MOVE mail loss, mbox self-copy panic, THREAD fixes, QRESYNC resync), mbox_lock_timeout 30s	no-body-in-particular	19 days ago

ffe7ec39	spamassassin r4 (close 0002 limit evasions, ARC cap, CNAME fix), opendkim r37 (MaximumHeaders), dovecot r4 (0030), cap-hit rules	no-body-in-particular	20 days ago
abd88d71	failure modes: OpenDKIM fail-open on non-SMTP path, mail-health monitoring, safer cert-renew	no-body-in-particular	20 days ago
32ffb26d	SMTPUTF8 casefold DKIM bypass fix, config-review fixes (fail2ban, Thunderbird path, SA anchors)	no-body-in-particular	20 days ago
0ee49fad	config round 3: recipient allow-list, own-domain spoof rejects, size/rate limits, DKIM SignHeaders, Dovecot limits/quota/TLS, nftables	no-body-in-particular	20 days ago

README.md

mail-hardening

Security fixes and Gentoo ebuilds for the mail stack on coredump.ws: **Postfix** 3.11.7, **Dovecot** 2.4.5, **SpamAssassin** 4.0.2, **OpenDKIM** 2.10.3 and Sendmail's libmilter 1.0.2.

The setup they were written for:

- Postfix receives on 25 (postscreen) and 587.
- Every inbound message passes through a SpamAssassin `content_filter` pipe and an OpenDKIM milter.
- Postfix `local(8)` delivers to mbox.
- Dovecot serves IMAP on 143/993 from those mbox files, with PAM and passwd auth. Its auth socket also backs Postfix SMTP AUTH.

How the fixes were found: twelve audits on 2026-10-07:

- source code review of each daemon;
- coverage-guided fuzzing;
- configuration and known-CVE checks;
- variant analysis;
- an adversarial review of the finished patches.

Each finding was reproduced on a private build (ASan/UBSan) before it was fixed. The audits, patches and tests were done with an AI model (Claude), directed and checked by the site's administrator; the patches carry a `Co-Authored-By` trailer saying so.

Status:

- **Dovecot:** several of these bugs are not fixed upstream as of 2026-10-07. They are marked below.
- **Postfix:** 3.11.7 is the current release and had already absorbed the 2026 audits. Its patches here are low severity, and none is reachable remotely in the setup above.

Using the overlay

`overlay/` is a Portage repository (`masters = gentoo`):

```
# /etc/portage/repos.conf/mail-hardening.conf
[mail-hardening]
location = /path/to/mail-hardening/overlay
```

What it contains:

Ebuild	Base	Changes
`mail-mta/postfix-3.11.7-r1`	`::gentoo` 3.11.7	The `::gentoo` ebuild plus a `PATCHES` array
`net-mail/dovecot-2.4.5-r4`	`::gentoo` 2.4.5-r1	The Gentoo patches, then ours
`mail-filter/spamassassin-4.0.2-r4`	`::gentoo` 4.0.2-r1	The Gentoo patches, then ours
`mail-filter/opendkim-2.10.3-r37`	`::gentoo` 2.10.3-r35	The Gentoo patches, then ours
`mail-filter/libmilter-1.0.2_p5-r1`	`::gentoo` 1.0.2_p5	The Gentoo patches, then ours

Notes:

- `KEYWORDS` is `amd64` only, because that is what was built and tested.
- Each `files/` directory also carries the `::gentoo` files the ebuild needs.
- All of them prepare and compile through Portage with the USE flags in use here:

- Postfix: `berkdb eai ldap lmdb mbox memcached pam sasl ssl`
- Dovecot: `lz4 pam zstd`
- OpenDKIM: `ssl`

Test suites

Each package's upstream test suite was run through Portage (`FEATURES=test`) on the patched source and on the stock `::gentoo` source, and the results compared:

Package	Patched	Stock
Dovecot (`make check`, 26 patches)	156 programs, 59,097 tests, 0 failed	same
Postfix (`make tests`, per directory)	5,131 PASS lines; identical failing targets	same
SpamAssassin	204 files, 2,795 tests, PASS	same
OpenDKIM (libopendkim)	156/156 pass	156/156 pass

Postfix: the ebuild has no `src_test`, and the top-level `make tests` stops at the first failing directory, so each `src/*` directory was run with `make -k tests`.

- **Timezone:** the cleanup/milter, postcat and bounce tests compare against output recorded in US Eastern time and need `TZ=America/New_York`. With it they all pass, patched and stock.
- **Failures left in both trees, all environmental:**
- `myaddrinfo_test`: the reference output is from a BSD host, with AF_INET6 = 28.
- `nullmx_test` and three `smtpd` tests do live DNS lookups.
- `dict_sqlite_test`: SQLite is not built.
- `byte_mask_test2` and `postmap file_test`.

SpamAssassin: Gentoo disables the spamd/spamc tests, so patch 0001 is covered by its own write-failure tests (see the patch header).

libmilter: has no test suite.

Every patch has a header that explains the bug, how to trigger it, and the fix.

Dovecot 2.4.5

Severity is for an internet-facing IMAP server with mbox storage.

Not fixed upstream (as of 2026-10-07):

Patch	Fix
0013 mbox-content-length-range	**High, remote, no authentication.** One email with `Content-Length: 9300000000000000000` makes every later sync of the recipient's mbox fail: `pread()` past `OFF_T_MAX`, then `SELECT INBOX` → `NO [SERVERBUG]` until the file is fixed by hand. A value of `2^64 - D` instead wraps back to an earlier `From` line and fails an assertion on every sync. Mailboxes already poisoned this way recover on the first sync after the patch.
0001 login-common STARTTLS	**Medium.** With `ssl = required`, a SASL initial response sent before STARTTLS stays buffered across STARTTLS. An attacker on the path can inject `AUTHENTICATE PLAIN <attacker credentials>` before the victim's STARTTLS. The victim's later `AUTHENTICATE PLAIN` without an initial response then logs into the **attacker's** mailbox, and the victim's TLS certificate check still passes. Affects 143 with STARTTLS, not 993. pop3-login (STLS, then AUTH PLAIN) is affected the same way; it was verified and is fixed by the same change.
0002 imap-login use-after-free	**Low-Medium, pre-auth.** Found independently by code review and by fuzzing. `a AUTHENTICATE PLAIN` followed by EOF, or an initial response over 8 KiB, destroys the client. The caller then reads `cmd_tag` from freed parser memory.
0014 mbox X-IMAPbase uid-last overflow	**Medium.** `X-IMAPbase: 1 4294967295` in the first mail of an empty or new mbox makes `next_uid` 0, so every open fails an assertion.
0010 auth tokens in debug log	**Low-Medium when** `auth_debug = yes`**.** The debug log shows the *expected* DOVECOT-TOKEN on a mismatch, and every issued token, without checking `auth_debug_passwords`. Anyone who can read the log can then get a successful DOVECOT-TOKEN authentication for any user on the 0666 `auth-token` socket. Mail access also needs the only service that accepts the token, imap-urlauth, behind `token-login/` (0750, login user only).
0011 passdb-pam fail delay	**Medium (DoS).** pam_unix's ~2 s `pam_fail_delay()` sleeps inside an auth-worker. Around 15 failed logins a second from anywhere ties up all 30 workers. A no-op `PAM_FAIL_DELAY` callback fixes it. **Behaviour change:** this also cancels a delay set on purpose with `pam_faildelay.so` (measured: 3.98 s down to 0.015 s). Only Dovecot's own non-blocking `auth_failure_delay` remains, and it doesn't limit concurrency, so total guessing throughput goes

Patch	Fix
	up. Rate-limit at the network level (fail2ban, `smtpd_client_auth_rate_limit`).
0004 NOTIFY fetch-ctx leak	Low. A failing `NOTIFY SET` leaks memory every time: 40 MB grew to 1.26 GB.
0003 imap-match grapheme clusters	Low. A LIST pattern with more than 64 KiB of combining marks fails an assertion.
0012 auth username_format	Hardening. A failed `auth_username_format` expansion was ignored.
0015 doveadm fetch text.utf8	Low. A header line without a name inside a MIME part fails an assertion in `doveadm fetch text.utf8`.
0019 istream-header-filter seek	Low. Seeking back to the current offset re-parsed the header from the wrong parent position: headers were lost, body bytes duplicated, and an assertion fails when the visible header is empty. Needs an mbox mail whose only headers are ones Dovecot hides (a user can APPEND one); found by fuzzing.
0020 subscriptions invalid UTF-8	Low (user self-DoS). An invalid UTF-8 line in the subscriptions file makes LSUB/LIST (SUBSCRIBED) fail an assertion; the entry is now dropped. Found by fuzzing.
0021 mbox X-UID wraps next_uid	**Medium, remote** (sibling of 0014). `X-IMAPbase: 1 4294967294` plus `X-UID: 4294967295` in the first mail of an empty or new mbox wraps `next_uid` to 0; every sync then fails `assertion failed: (sync_ctx->next_uid != 0)`, so the mailbox can't be opened. Now it renumbers instead. The `config/postfix/mbox_header_checks` filter blocks it too.
0022 auth CPID reconnect double free	Low-Medium. A login process reconnecting with the same CPID while its old connection is at EOF frees the old connection twice, crashing auth (all in-flight IMAP logins and SMTP AUTH fail). Needs access to the login socket, not the network.
0023 master passdb debug logs	Low-Medium. With `auth_debug = yes` and `auth_debug_passwords = no`, "passdb out" on the auth master socket, and three lib-auth-client debug lines, still logged `pass=` fields.
0024 imap-hibernate auth_token	Low. With debug logging and IMAP hibernation, `auth_token` was logged (variant of 0010).
0025 SEARCHRES search-args leak	Low, logged-in user. A SEARCH that waits for an ambiguous `$` leaked its search args: 12 MB to 285 MB over 4000 pipelined

Patch	Fix
	pairs.
0027 mbox NUL in header name	Low, logged-in user. `str_append()` stopped at a NUL in a header name, so header rewrites landed up to k bytes early and overwrote X-UID/Status. Postfix rejects such headers, so it is not reachable remotely.
0028 mbox From_ at body start	Low-Medium, logged-in user. When a body starts with a valid `From` line, the body size left out the separating empty line, so expunging moved or left one byte wrong and corrupted neighbouring mail.
0029 mbox valid-From at buffer boundary	Low-Medium, logged-in user. A correct Content-Length was rejected whenever the next `From` line crossed the 8 KiB read buffer. A saved mail with `From` in its body then split into two, with the second taking its headers from the body. It depends only on byte offsets, so an unrelated expunge can trigger it.
0030 imap-master auth_token in debug log	Low. With `-D`, the unhibernation line (including `auth_token=`) was logged; 0024 missed this path.
0031 MOVE within the same mailbox loses mail	**Medium, silent mail loss.** If `UID MOVE` into the *same* mailbox fails partway (another session expunged one UID → `NO [EXPUNGEISSUED]`, a lock timeout, or a full disk), the copies are rolled back but the source transaction, with the expunges of the messages already moved, is still committed. Reproduced every time. Not fixed upstream.
0032 mbox COPY within the same mailbox	Low-Medium. COPY/MOVE into the same mbox while another session appends panics at `istream-raw-mbox.c:183`; the copy now locks and syncs before opening the source. Not fixed upstream.
0035 THREAD placeholder parents O(N²)	Low, remote. A chain of placeholder parents made every THREAD quadratic (60k messages: 7.2 s); now linear, with identical output. Not fixed upstream.
0036 QRESYNC after modseq reset	Low. mbox keeps UIDVALIDITY in the file but modseqs only in the index; after an index rebuild HIGHESTMODSEQ dropped and QRESYNC clients silently missed changes. Now a full resync is sent.

Backports from dovecot/core `main`:

Patch	Upstream commits	Fix
0016 auth reject empty passwords	6fac3e2f, f43224e2, 268215a2, b2b2d74e	Empty client passwords reached PAM. With `pam_unix nullok`, that is a pre-auth login. Empty client passwords are now rejected for every passdb, including `nopassword` users.
0017 ssl-iostream busy loop	2742928e, ccaa874f	An unauthenticated client can make the TLS output stream busy-loop the CPU during the handshake.
0005 FETCH PREVIEW out-of-bounds read	a00c7cd4	`FETCH 1 (PREVIEW (LAZY LAZY))` reads past the end of the arguments.
0006 SEARCH nesting depth	4f181e89, c7c40d8c	About 25,000 nested `(` overflow the stack.
0007 SEARCH INTHREAD crashes	9d8b272d, d4ee7d9e, 9ecc89d1	Crashes with ORDEREDSUBJECT, NOT and OR.
0008 SEARCH MIMEPART crashes	d1bb5a6c, cf8da498	`MIMEPART (PARENT …)` crash; also makes several MIMEPART keys combine correctly.
0009 APPEND CATENATE failure	12dc7b0a	Crash when saving fails partway.
0018 mbox From_ year out-of-bounds read	f9f517ee	Out-of-bounds read of the year in the `From` line.
0026 lib-index ext-hdr-update offset overflow	653b02c7, plus a unit test	uint32 `offset + size` wrap in a user's own `dovecot.index.log`.
0033 THREAD without recursion	0ac4d69, b0a8597	Remote mail where each message replies to the next one's future Message-ID got past the ancestor cap, and THREAD REFERENCES overflowed the stack (~95k messages).
0034 thread strmap remap panic	14b19a6	Duplicate Message-IDs plus mail without one, then THREAD in two sessions: panic.

Patches 0003–0009 (and 0031, 0032) need a logged-in user, and they only crash or exhaust that user's own process. **0015** only affects an administrator running `doveadm fetch`. Upstream's unit tests for 0006 and 0007 are not included.

Postfix 3.11.7

Patch	Fix
0001 smtpd stale MAIL parameters	Low. SIZE= and AUTH= from a rejected `MAIL FROM` are kept. The next MAIL then gets a wrong 552 or "503 multiple AUTH=", and a stale AUTH= reaches the queue file, the policy service and the milter `{auth_author}`.
0002 stand-alone size check	Hardening. `sendmail -bs` with an oversized SIZE= dereferences NULL in the user's own smtpd. Stand-alone mode now checks SIZE= against `message_size_limit` itself and still replies 552.
0003 mbox From_ sender quoting	Low, local only. `sendmail -f 'a@[1 Mon Jan 01]'` produces a `From` line that Dovecot rejects. The message then merges into the previous one (content spoofing), or INBOX becomes unreadable. smtpd already rejects these senders.
0004 MIME-Error before the append pointer	Low. With `non_empty_end_of_header_action = add_header`, the header was written where milters can't see it.
0005 cleanup unknown client flags	Hardening backport from 3.12 snapshots (stricter than upstream: 3.11.7 uses flags only up to bit 10).
0006 TLS limits fail closed	Low, config only. An empty version in `smtpd_tls_protocols` was taken as "no limit", so `">= TLSv1.2"` (with a space) meant TLS 1.2 only, and a bare `>=` meant no floor. A numeric version OpenSSL rejects (`>=0x0305`) left the server with no floor at all, accepting TLS 1.0/1.1. Now such values log a warning and disable TLS. **At security level `may` this means no STARTTLS**, the same as upstream does for other invalid protocol lists. Valid spellings (`>=TLSv1.2`, `!SSLv2, !SSLv3`, `TLSv1.2 TLSv1.3`, `>=TLSv1.2 <=TLSv1.3`) are unchanged (tested). Not upstream.
0007 `-V` log tag use-after-free	Debug only. With `-V` and `-o syslog_name=…`, the stderr logger keeps a pointer into a buffer that is reallocated after the config loads. Not upstream.
0008 TLS scache/DANE/tlsmgr	Backport of three 3.12 fixes (session-cache decode accepting colons, tlsmgr replying with stale data, a fingerprint leak), plus a fix for a panic on a one-

Patch	Fix
	character `smtp_tls_fingerprint_cert_match` value, which is still in upstream.
0009 milter aborted body replacement	Backport from 3.12 (20260821). A milter that disconnects after SMFIR_REPLBODY made Postfix commit a corrupt queue file under `milter_default_action = accept`.
0010 milter macro override list	Low. A milter that overrides macros leaks and keeps a stale list on every reconnect. Not upstream.
0011 ip_match octet overflow	Config only. Signed overflow parsing a DNSBL reply filter octet. Not upstream.
0012 regexp/pcre `$n` overflow	Config only. `atoi()` made `$4294967297` mean `$1`. Not upstream.

SpamAssassin 4.0.2

Patch	Fix
0001 spamc output write error	**High in a content_filter.** `spamc` exits 0 when writing its output fails (ENOSPC/EFBIG). A filter script trusting the exit code re-injects the truncated message; tested under a 100 KiB file-size limit with 433,042 bytes in and 102,400 out. Now it exits `EX_IOERR` (74), also in BSMTP mode (`-B`), and libspamc's `message_process()` returns `EX_IOERR` instead of writing the message a second time.

| 0002 bound per-message work | **High.** One crafted message can make a scan hit `time_limit`, and the verdict then counts only the rules that ran. In tests that gave a score of 0.0, so spam was delivered as ham, and five such messages at once stalled all scanning. The patch bounds each of the cases below, and the worst 5 MB message now takes about 12 s. Measured costs and limits:
- **Per-URI-host CNAME lookups.** No limit and 3 s each: 40 URIs on a silent name server took 91 s. Now `dns_max_cname_cache` 10, stopping at the first timeout.
- **O(n²) HTML tag nesting.** Over 50 s for 466 KB, now 1.3 s.
- **No total limit on body text across parts.** About 95 parts of 50 KB took 85 s. Now `body_total_scan_size`.
- **Up to 50 DKIM signatures,** each re-hashing the body: 38 s. Now `dkim_max_signatures` 5.
- **Unlimited header fields.** 53 s and 782 MB.
- **Unlimited URIs.** 37 s. Now 2000. |

Also, on stock: `score TIME_LIMIT_EXCEEDED 3.0`, so an aborted scan is not a free pass. SpamAssassin's test suite passes with both patches: 2,795 tests, the same as stock.

| 0003 close scan bypasses from 0002's limits | **High.** A review found the 0002 limits could be triggered on purpose to hide spam, and 0003 closes each case:
- **Header field cap:** 5,000 junk header fields in front of the real ones scored 82 → 0. The fields that matter are now kept past the cap.
- **Total body limit:** a 310 KB filler part first meant later parts were never scanned or rendered. Every part is now rendered, and the budget is split between parts.
- **URI cap:** the HTML cap didn't apply to links, and a random 2000 URIs were kept. Fixed, with a separate flag.
- **ARC:** 50 ARC sets got around the DKIM limit (`arc_max_instances` 10).
- **Author signatures:** the author-domain signature is kept within `dkim_max_signatures`.
- **CNAME lookups:** they stopped after the first answered host. Fixed.
`spamassassin/27_cap_hits.cf` scores every cap that is hit. Test suite: 2,795 PASS. |

OpenDKIM 2.10.3

Patch	Fix
0001 don't truncate envelope recipients	**Medium-High in a re-injecting setup.** `mlfi_envrcpt` copied each recipient into a 256-byte buffer, so a longer recipient never matched an end-anchored `DontSignMailTo` pattern. With Postfix's percent hack, `admin%example.org%…@example.org` still delivers locally, so inbound mail with a forged `From:` of your domain got signed. Not fixed upstream.
0002 decide MaximumHeaders at EOH	Medium. Over 64 KiB of headers applied `On-Security` (tempfail) before OpenDKIM knew whether it would sign, so inbound mail re-injected by a filter sat in the maildrop forever. Now it is decided at end of headers, and mail to a `DontSignMailTo` recipient is accepted in sign-only mode. Not fixed upstream.
0003 bound header-name termination	Low here, High in general. `dkim_header()` wrote a NUL at `name[field_name_length]` into a 4097-byte stack buffer; a field name of 18,000+ bytes crashed stock opendkim. Postfix's `line_length_limit = 2048` keeps it out of reach. Not fixed upstream.
0004 no A-R header in sign-only mode	Backport of upstream a6665347.
0005 decide MaximumHeaders when signing is known	0002 still deferred oversized-header mail from external clients, which a sign-only filter never signs. The limit now applies only once OpenDKIM knows it will sign. Test suite 156/156.

libmilter 1.0.2_p5

Patch	Fix
0001 bound smfi_getsymval and the argv decoders	Low, MTA side only. A macro packet with an odd number of strings made `smfi_getsymval()` walk past the argv NULL (SEGV in the filter); `dec_argv` accepted an unterminated last string; `st_connectinfo` read one byte past the packet. Not in sendmail 8.18.2's release notes.

Configuration

These problems needed configuration changes, not code. The files are in `config/`.

1. **Mbox metadata headers from outside.** `postfix/mbox_header_checks`, set as `header_checks`, strips `Content-Length`, `Status`, `X-Status`, `X-Keywords`, `X-UID`, `X-IMAP` and `X-IMAPbase`. It also matches the forms with whitespace before the colon (`X-Status : D`), which both Postfix and Dovecot accept as the same header. The first version missed them.
2. **Why:** `local(8)` mbox delivery keeps them, and Dovecot then trusts them.
3. **What it blocks:** - Dovecot 0013 and 0014. - A correctly sized Content-Length that hides the mails after it. - Senders presetting `\Seen \Deleted NonJunk` on their own mail.
4. **Where else it applies:** to any mbox setup with Postfix local delivery, patched or not. Dovecot's own save path drops the same headers.
5. **DKIM signing of inbound mail.** A filter that re-injects with `sendmail` makes every inbound message reach `non_smtpd_milters` as localhost. If OpenDKIM's `InternalHosts` has 127.0.0.1 and `SigningTable` covers your domain, an outside sender's `From: you@yourdomain` gets **signed with your key**. A bounce returns the signed copy, which can then be replayed with DMARC passing.
6. **Fix (r7, 2026-10-08, supersedes the DontSignMailTo domain entries):** `bin/spamfilter` re-injects over SMTP to a dedicated `127.0.0.1:10026` smtpd with `-o smtpd_milters= -o receive_override_options=no_milters` (`postfix/master-reinject.cf`), so inbound mail never reaches OpenDKIM at all. An nftables output rule lets only root and spamd (by numeric uid) connect to 10026, which has no content filter. The old fix, `DontSignMailTo` with the local domain, skipped signing whenever *any* recipient was local, so outbound mail with a local Cc/Bcc went out unsigned; `*@yourdomain` and `*@yourdomain.w*` are gone from it.
7. **Test:** `monitoring/milter-probe.py SOCKET CLIENT_IP ENV_FROM HDR_FROM RCPTS [AUTH]` asks the live OpenDKIM whether it would sign, without queueing mail.

Expected after r7: authenticated or local submission to local+remote recipients SIGNED; an outside client with a forged own-domain From UNSIGNED; address literals UNSIGNED. With the old DontSignMailTo the local+remote case printed UNSIGNED.

8. **Fix:** `-o smtpd_milters=` and `-o receive_override_options=no_address_mappings` on the filtered smtpd.
9. **Fix:** `DontSignMailTo` must also cover address literals (`*@\[*`). Postfix treats `user@[your.ip]` as local.
10. **Fix:** `postfix/recipient_checks` first in the port-25 recipient restrictions. It rejects address literals and recipients of 200 characters or more, which OpenDKIM would truncate (OpenDKIM 0001). Also set `allow_percent_hack = no` and `swap_bangpath = no`.
11. **Fix:** `On-Security accept` in opendkim.conf, until OpenDKIM 0002 is installed.
12. `bin/spamfilter`, a content_filter pipe script:
13. It uses `spamc -x` so a down spamd defers mail instead of passing it unscanned.
14. It refuses truncated output.
15. It keeps a bounce's null sender. Use `null_sender=` in master.cf; without it, pipe(8) turns `<>` into `MAILER-DAEMON`.
16. It strips forged `X-Spam-*` headers and forged `Authentication-Results` that claim your authserv-id.
17. It uses `--` before recipients.
18. `pam.d/dovecot-mail`. `passdb pam { service_name = login }` exposes the local-login stack to the internet:
19. `pam_faillock`: three bad IMAP or SMTP passwords lock that account out of console, sudo and ssh too.
20. `pam_unix nullok`: empty passwords are accepted.
21. Root can be guessed without limit and gives "Logged in, but initialization failed" when the password is right.
22. **Fix:** use a dedicated service limited to mail users.
23. **Postfix.**
24. Leave `smtpd_sasl_auth_enable` off globally and turn it on only for submission, together with `smtpd_tls_auth_only = yes`. Dovecot enforces cleartext rules only in its login processes, not on the auth socket Postfix uses.
25. Set `smtpd_client_auth_rate_limit`.
26. Bind sender to login on 587 with `postfix/sender_login` and `reject_sender_login_mismatch`.
27. Require TLS 1.2 or later, and send the full chain (`smtpd_tls_chain_files`).

More configuration (later audits, 2026-10-07)

1. **MIME that SpamAssassin and Dovecot parse differently.** Nine constructions let a part reach the mailbox unscanned while Dovecot serves it as a normal text part:
2. two `Content-Type` or `Content-Transfer-Encoding` fields;
3. RFC 2231 `boundary*0=` next to `boundary=`;
4. an encoded word in the boundary;
5. an unquoted boundary with trailing text;
6. a quoted-pair in the boundary;
7. a `--BOUNDARYx` prefix line;
8. `multipart` without a subtype.

Fixes:

- `postfix/inbound_header_checks`, on a `cleanup-in` service used only by the port-25 smtpd, rejects five of them at SMTP time.
- `spamassassin/20_mime_ambiguity.cf` scores the rest.
- `body_part_scan_size 300000` and `rawbody_part_scan_size 1000000`, because SpamAssassin scanned only the first 50 KB of each text part.
- **Re-injection rewrote header addresses after the scan.** `From: ceo` became `From: ceo@yourdomain` once spamd had already scored it. `bin/spamfilter` now re-injects with `sendmail -G`. Its Authentication-Results stripping also handles comments and quotes around the authserv-id.
- **A forged** `Delivered-To:` **for our own domain made local(8) bounce "mail forwarding loop" to the forgeable sender** (backscatter). `inbound_header_checks` rejects it.
- **fail2ban** (`fail2ban/`):
- The stock `sshd` filter accepts "on <anything>" after the address, and sshd logs usernames verbatim. A username like `x VICTIM-IP on` therefore gets VICTIM-IP banned. `sshd.local` closes this.
- `dovecot24.conf` replaces a dovecot filter that never matched Dovecot 2.4 lines.
- There are new postscreen and recipient_checks jails, and `ignoreip` is set explicitly.
- Old Dovecot `auth_verbose_passwords` lines may survive in freed pages of `fail2ban.sqlite3`: `VACUUM` it.

Round 3 (2026-10-08): attack paths, auth, resources, recipients, spoofing

1. **Backscatter through system accounts.** Every /etc/passwd account was a valid recipient. Mail to `bin@` failed delivery and was bounced, content included, to the forged sender. Fixes: - `local_recipient_maps` is now an explicit list

(`postfix/local_recipients`) plus aliases, and `abuse:` was added. - On port 25, DSN and ETRN are discarded, `@localhost` and `mailer-daemon@` are rejected, and at most 20 recipients are accepted per message.

2. **Own-domain spoofing from outside.** A plain `From: admin@yourdomain` scored about 2 despite `p=reject`. Fixes: - `postfix/own_domain_senders` and `postfix/helo_access` reject our domain as envelope sender and HELO from unauthenticated clients. - `spamassassin/25_own_domain_spoof.cf` scores our domain in From without our DKIM, multiple From addresses, our address in the display name, and lookalikes. - OpenDKIM now signs and oversigns `Content-Type`, `Message-ID`, `To`, `Subject` and the other important headers. Before, only `From` was oversigned, so a signed message could have its Content-Type changed and be replayed.
3. **Disk fill and queue starvation.** One filesystem, with 100 MB messages fanning out to many mailbox copies. Fixes: - Limits: `message_size_limit` 50 MB, `mailbox_size_limit` 4 GB, `queue_minfree` 10 GB. - Per-IP message, recipient and connection rate limits, and shorter queue lifetimes. - Shorter spamd timeouts (`time_limit 25`, `--timeout-child=40`, `spamc -t 60`). - spamfilter uses its own temp dir with a free-space guard (`bin/spamfilter`).
4. **IMAP/SMTP AUTH and sessions.** Fixes: - Dovecot: imap-login `process_limit 512`, imap `process_limit 128` and `vsz_limit 1G`, and a count quota (`dovecot/limits-quota-tls.conf`). - nftables per-IP limits on 143/587/993 (`nftables/mailguard.nft`). - `check_sasl_access` stops the reports-only `dmarc` login from sending. - TLS: submission excludes aNULL/kRSA/SHA1 suites, and Dovecot is limited to TLS 1.2 ECDHE+AEAD with no tickets. - Still recommended: a mail-only password, separate from the system password.

1. **SMTPUTF8 casefolding (critical).** With `smtputf8_enable = yes`, the default at compatibility_level 3.11, Postfix ICU-casefolds lookups. `admin@yourdomain.w\u017f`, with U+017F LONG S, is then local to Postfix, but OpenDKIM's byte match in DontSignMailTo misses it. An outsider got arbitrary content DKIM-signed, and a crafted loop bounce returned the signed copy. Fixes: - `smtputf8_enable = no`. - A non-ASCII `Delivered-To` reject in `inbound_header_checks`. - `DontSignMailTo` also matched `*@yourdomain.w*` and `*@localho*` (`*@yourdomain.w*` removed in r7: re-injected mail no longer passes the milter). - `spamassassin/26_display_name_obfuscation.cf` catches display names obfuscated with bidi controls, zero-width characters, fullwidth forms or homoglyphs.
2. **Config review fixes.** - **fail2ban:** `pam-generic` ignores `tty=dovecot`, so IMAP password typos are handled by the mail-port-only dovecot jail and don't trigger a 14-day all-ports ban. The 5.1.1 threshold is 10 (`fail2ban/jail.d/17-a25.local`). - **Local senders on port 25:** mail from local

clients on port 25 (a desktop Thunderbird) has no recipient cap, and the MIME rejects apply only to top-level headers, so abuse reports with spam attached still go out. - **SA rules:** the duplicate-header rules are anchored so they don't fire on quoted body text. Copies of your own posts that come back through a mailing list score 3 instead of 6 (`25b_own_domain_list.cf`). - **HELO:** a trailing dot in HELO is matched.

1. **Silent failure modes.** - **OpenDKIM down or hung:** every message entering through sendmail/pickup sat in the maildrop for good. That includes cron mail, local sendmail, and all inbound mail re-injected by the filter: no bounce, no alert. Fix: `non_smtpd_milters = { unix:/run/opendkim/opendkim.sock, default_action=accept }`. There must be no spaces around `=` inside the braces; with spaces every cleanup dies. - **Monitoring:** `monitoring/mail-health` runs from root's cron every 5 min. It checks spamd PING, the OpenDKIM handshake, the local resolver and DNSBL, maildrop age, the deferred queue and free space. Hourly, it sends a GTUBE probe from port 25 to a local-only `mailhealth` alias pipe (`monitoring/mail-health-sink`, which runs as nobody), and the probe must arrive scanned. Problems go to syslog at mail.crit and to a sticky ALERT file. - `bin/cert-renew`: it now refuses a certificate that is expired, doesn't match its key, or is for the wrong host. It replaces `/etc/cert.pem` atomically and keeps its ACLs. It reloads Postfix and Dovecot instead of restarting them; a restart cut a message being appended and caused a duplicate.

Not included

- **Header-name registry growth (Dovecot):** `FETCH BODY.PEEK[HEADER.FIELDS (...)]` with hundreds of new header names, repeated, grows the user's own imap process without bound (`vsz_limit` caps it). A fix needs a design change, so there is no patch.
- **More upstream SEARCH fixes:** ca876ad14 and the `mail_search_args_simplify` series fix a `SEARCH 5*:8*:3 3` assertion; not backported.
-

The proof-of-concept scripts used to verify these bugs are not published.

License

GPL-3.0-or-later, see **LICENSE**. The exception is the ebuilds and init scripts that are modified copies of Gentoo's: they are Gentoo's work under GPL-2, as their headers say, and stay that way. The patches are also offered under the licence of the project they patch, so they can go upstream (Postfix: IPL-

1.0/EPL-2.0, Dovecot: LGPL-2.1/MIT, SpamAssassin: Apache-2.0, OpenDKIM and libmilter: BSD/Sendmail). `upstream/opendkim-develop/` is OpenDKIM's code under its own licence.