Message-ID: <87mryccisi.fsf@gentoo.org>
Date: Wed, 06 May 2026 22:47:09 +0100
From: Sam James <sam@...too.org>
To: oss-security@...ts.openwall.com
Subject: Vulnerability fixes in Tor 0.4.9.7

From diffing 0.4.9.6 and 0.4.9.7 [0]:

```
+Changes in version 0.4.9.7 - 2026-05-06
+  This is a security release fixing several major bugfixes that were reported
+  in the past weeks. Huge thanks to everyone that reported these issues! We
+  strongly recommend upgrading as soon as possible.
+
+  o Major bugfixes (cell handling):
+    - Fix out-of-bounds read (OOB) when END, TRUNCATE and TRUNCATED cell
+      have no reason in their payload. TROVE-2026-011. Found by Found by
+      Brian Carpenter (geeknik). Fixes bug 41254; bugfix
+      on 0.1.1.1-alpha.
+
+  o Major bugfixes (conflux):
+    - Do not attempt or accept BEGIN_DIR via conflux legs. TROVE-2026-
+      008. Credit to Anas Cherni from Calif.io in collaboration with
+      Claude and Anthropic Research. Fixes bug 41243; bugfix
+      on 0.4.8.1-alpha.
+
+  o Major bugfixes (conflux, relay):
+    - Adjust conflux out-of-order queue accounting when clearing a
+      queue. TROVE-2026-010. Found by aptupdate. Fixes bug 41251; bugfix
+      on 0.4.8.1-alpha.
+
+  o Major bugfixes (pathbias):
+    - Fix a client-side crash caused by double-close of a circuit while
+      under circuit queue memory pressure. TROVE-2026-009. Found by
+      cypherpunks. Fixes bug 41237; bugfix on 0.3.3.6-rc.
+
+  o Major bugfixes (relay):
+    - Fix null pointer dereference when receiving a CERT cell out of
+      order. TROVE-2026-006. Found by Fwame. Fixes bug 41240; bugfix
+      on 0.2.4.4-alpha.
+
+  o Major bugfixes (relay, onion service):
+    - Fix off-by-one out-of-bounds read if a malformed BEGIN cell is
+      received. TROVE-2026-007. Found by Flanagan. Fixes bug 41245;
+      bugfix on 0.2.4.7-alpha.
+
+  o Minor features (fallbackdir):
+    - Regenerate fallback directories generated on May 06, 2026.
+
+  o Minor features (geoip data):
+    - Update the geoip files to match the IPFire Location Database, as
+      retrieved on 2026/05/06.
+
```

The referenced bugs are private, so no more details are available
yet. There were several recent other security releases too for Tor.

[0] https://gitlab.torproject.org/tpo/core/tor/-/blob/tor-0.4.9.7/ReleaseNotes#L5

Download attachment "signature.asc" **of type** "application/pgp-signature" **(419 bytes)**