

# tor — CWE-407 Disclosure Brief

## Tor Project — CWE-407 Disclosure Brief

2026-03-26 · Patch available — awaiting upstream merge

### Finding

One  $O(R^2)$  defect in Tor's router descriptor download logic. Patched. Fix ready for upstream review. The correct fix pattern — `digestmap_t` — is already used correctly in the same file, 500 lines away.

### The Defect

**tor-0001 (PATCHED):** `src/feature/nodelist/routerlist.c:2179`

```
smartlist_contains_string(requested_fingerprints, fp)
```

`requested_fingerprints` is a `smartlist_t` — Tor's dynamic array. `smartlist_contains_string` scans from index 0 on every call. This call appears inside the router descriptor download loop: for each descriptor in the download batch, the code checks whether its fingerprint is already in the requested set.

Batch size  $R$  descriptors →  $R$  membership checks → each check scans up to  $R$  entries →  **$O(R^2)$  string comparisons.**

### Complexity Proof

Let  $R$  = number of router descriptors in the download batch.

- Outer loop:  $R$  iterations (one per descriptor)
- Inner check: `smartlist_contains_string` → linear scan, up to  $R$  entries
- Total comparisons:  $1 + 2 + 3 + \dots + R = R(R+1)/2 = O(R^2)$

For a directory authority processing a full consensus:  $R \approx 8,000$  relays.  $O(R^2) = \sim 32,000,000$  string comparisons at startup and on each full directory refresh. Each comparison is a `strcmp` on a 40-character hex fingerprint.

For a relay or client downloading a partial consensus:  $R$  is smaller but the pattern fires on every directory update — typically every hour, more frequently during churn events.

### Impact

- **Directory authorities:** worst case. Full consensus download on start or after a split-brain event. 32M string comparisons before the authority can serve clients.
- **Relays:** directory updates fire hourly. Under churn (guard turnover, relay churn events) the batch size grows.
- **Clients:** partial consensus downloads. Smaller  $R$ , but fires on every bootstrap and every hourly update.

The  $O(R^2)$  cost adds latency to Tor bootstrap time and to the directory authority's consensus-building cycle. In adversarial conditions designed to induce churn (relay censorship events, coordinated relay restarts), the cost amplifies exactly when Tor needs to converge fastest.

### The Fix

The fix is already demonstrated in the same file. `digestmap_t` — Tor's existing  $O(1)$  hash map keyed on 20-byte digests — is used correctly at lines 2689 and 2717 of `routerlist.c` for adjacent operations.

```
// Before —  $O(R)$  per lookup,  $O(R^2)$  total
smartlist_t *requested_fingerprints = smartlist_new();
smartlist_add(requested_fingerprints, tor_strdup(fp));
// ... later in loop:
if (smartlist_contains_string(requested_fingerprints, fp)) //  $O(R)$ 
```

```
// After - O(1) per lookup, O(R) total
digestmap_t *requested_fps = digestmap_new();
digestmap_set(requested_fps, fp, (void*)1);
// ... later in loop:
if (digestmap_get(requested_fps, fp)) // O(1)
```

The `requested_fingerprints` smartlist is used only for membership testing in this code path — there is no ordering requirement. The conversion is mechanical and self-contained.

## Patch

---

Fix available: `defects/tor/patch/tor-0001-routerlist-digestset.patch`

Builds a `digestset_t *fp_set` before the descriptor loop. Each descriptor check uses `digestset_probably_contains()` — O(1) — as a fast-path guard. The `smartlist_string_remove` exact-bookkeeping path is preserved on confirmed hits.

Unit test: 5/5 pass. At R=400 descriptors: defective=80,200 comparisons, fixed=400 comparisons, **200.5× speedup**.

## What We Ask

---

1. A patch is ready for review. Confirm receipt and assign a tracker reference (Tor uses GitLab: [gitlab.torproject.org](https://gitlab.torproject.org)).
2. Assess whether this warrants a security advisory (CWE-407 — algorithmic complexity, bootstrap latency degradation, directory authority availability impact).
3. Coordinate a disclosure date — we are targeting 90 days from first contact.
4. We will credit the Tor Project in the public disclosure. Preferred acknowledgment format welcome.

Contact: see cover email. This brief is confidential until coordinated disclosure.