Buoyant Security Advisory 2025-01: Linkerd proxy metrics resource exhaustion (CVE-2025-43915)

Description

Linkerd proxies track and provide metrics for a workload's inbound and outbound HTTP requests. Inbound request metrics include an `authority` label, and outbound request metrics include a `hostname` label. Linkerd proxies that receive requests with a large number of unique hostnames may exhibit a corresponding high cardinality of metrics data. At the extreme, this metric data may consume a large amount of proxy memory, overwhelm metrics ingestion infrastructure, or create undesirable costs for third-party metrics ingestors.

Inbound `authority` Labels

Edge releases prior to edge-25.2.1, and Buoyant Enterprise for Linkerd releases 2.13.0–2.13.7, 2.14.0–2.14.10, 2.15.0–2.15.7, 2.16.0–2.16.4, and 2.17.0–2.17.1 track and expose Prometheus metrics that include an `authority` label for inbound requests. Users of affected versions should consult the Mitigation and Action Required sections below.

Outbound `hostname` Labels

Edge releases edge-24.10.3 through edge-25.1.2, and Buoyant Enterprise for Linkerd releases 2.17.0 and 2.17.1, track and expose Prometheus metrics that include a `hostname` label for outbound requests. Users of affected versions should consult the Mitigation and Action Required sections below.

Who is affected?

Generally speaking, Linkerd proxies that are exposed to HTTP traffic with unconstrained URLs are affected by this CVE. Common examples include:

- Linkerd deployments exposed to the Internet, e.g. through meshed ingress controllers.
- Linkerd deployments that take requests from arbitrary (i.e. uncontrolled) third-party applications.
- Linkerd deployments that mesh arbitrary third-party applications and have egress metrics enabled.

In these cases, malicious URLs can be crafted by attackers to increase proxy memory consumption over time.

Mitigation

Ensure that Linkerd proxies are not exposed to HTTP requests that contain an unbounded number of unique hostnames. For example, meshed workloads that handle Internet-facing traffic may need to have HTTP requests filtered before they hit the Linkerd proxy. Similarly, meshed workloads that make egress calls may need to be audited to ensure the number of unique hostnames is bounded.

Alternatively, update to the versions specified in the Action Required section below, which disable these metric labels by default.

Action Required

If mitigation is not possible and Linkerd proxies cannot be prevented from exposure to an unbounded number of unique hostnames, Linkerd should be updated. Users of edge releases should update to edge-25.2.1 or later. Users of Buoyant Enterprise for Linkerd should update to BEL releases 2.16.5, 2.17.2, 2.18.0, or later releases.

CWE

CWE-770: Allocation of Resources Without Limits or Throttling

CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L/E:P/RL:O/RC:C

CVSS Temporal Score

5.2

Credits

John Howard