HCSEC-2026-11 - Boundary Workers Vulnerable to Denial of Service During TLS Handshake

security-boundary

---

mark.collao 1 May 4, 2026, 9:39pm

Bulletin ID: HCSEC-2026-11
Affected Products / Versions: Boundary Community Edition and Boundary Enterprise up to 0.21.2, 0.20.2, 0.19.4, fixed in 0.21.3, 0.20.3, 0.19.5
Publication Date: May 4th, 2026

Summary
Boundary Community Edition and Boundary Enterprise (“Boundary”) workers are vulnerable to a denial-of-service condition during node enrollment TLS handshakes. An attacker with network access to the worker authentication listener may open a connection and delay or withhold the client certificate during the TLS handshake, causing worker connection handling to block. This may prevent legitimate worker connections from being accepted or routed. This vulnerability, CVE-2026-7776, is fixed in Boundary 0.21.3, 0.20.3, 0.19.5.

Background
Boundary workers use node enrollment to authenticate and establish trusted connections between Boundary components. During this process, Boundary performs a mutual TLS handshake and uses the negotiated TLS state and client metadata to route the connection appropriately.

Details
Boundary’s node enrollment dependency performed the server-side TLS handshake synchronously while accepting and classifying worker connections. A client that connected to the worker authentication listener and then stalled during the TLS handshake, including by delaying or not providing a requested client certificate, could block the connection handling path.

This could cause later legitimate worker connections to be delayed or prevented from completing, resulting in a denial of service for worker authentication and enrollment workflows. The issue requires network-level access to the affected listener, but does not require successful authentication.

Remediation
Customers should evaluate the risk associated with this issue and consider upgrading to Boundary Community Edition or Boundary Enterprise 0.21.3, 0.20.3, 0.19.5.

Please refer to Boundary’s upgrade documentation for general guidance: **Upgrade and database migration | Boundary | HashiCorp Developer** .

Acknowledgement

This issue was identified by the Boundary Engineering team.

We deeply appreciate any effort to coordinate disclosure of security vulnerabilities. For information about security at HashiCorp and the reporting of security vulnerabilities, please see ***https://hashicorp.com/security****.*

Related topics

Topic	Replies	Activity
Error tls handshaking connection on client: remote error: tls: internal error hcp	0	September 17, 2024
HCSEC-2024-02 - Boundary Vulnerable to Session Hijacking Through TLS Certificate Tampering security-boundary	0	February 5, 2024
TLS Handshake Error with Boundary Deployed in Nomad Cluster consul-nomad	3	May 9, 2022
Boundary worker proxy	2	April 5, 2021
Cannot disable TLS comms between worker and controller: "tls: first record does not look like a TLS handshake"	2	May 31, 2022