INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:48 UTC

# CVE-2026-48764: Server-Side Request Forgery in baptisteArno typebot.io

CVE VULNERABILITY | HIGH | CVSS 8.6

| | |
|---|---|
| SCC Item ID | SCC-CVE-2026-0334 |
| Type | CVE Vulnerability |
| CVE ID | CVE-2026-48764 |
| Severity | HIGH |
| CVSS Base Score | 8.6 |
| Affected Products | baptisteArno typebot.io (specific version unconfirmed, source: gemini discovery, secondary tier) |
| Published | 2026-06-17 |
| Discovery Source | Gemini |

## Executive Summary

A Server-Side Request Forgery vulnerability (CVE-2026-48764, CWE-918) has been reported in Typebot (baptisteArno/typebot.io), an open-source chatbot builder platform. If exploited, an attacker could force the typebot server to issue internal HTTP requests, potentially reaching cloud metadata endpoints, internal APIs, or configuration services not intended to be externally accessible. The affected version range is unconfirmed from authoritative sources; organizations running self-hosted typebot deployments should treat this as a priority pending vendor confirmation.

## Technical Analysis

CVE-2026-48764 describes a Server-Side Request Forgery condition (CWE-918) in Typebot (baptisteArno/typebot.io). The vulnerability appears to reside in the platform's HTTP request and script execution components, based on corroborating references from cvefeed.io and radar.offseq.com. SSRF in this context would permit an attacker to manipulate server-side HTTP request logic to reach internal network resources, cloud instance metadata services (e.g., AWS IMDSv1 at 169.254.169.254), or other services on the server's internal network. MITRE technique mappings include T1090.002 (Proxy: External Proxy) and T1071.001 (Application Layer Protocol: Web Protocols), consistent with SSRF-driven lateral movement and data exfiltration patterns. A CVSS base score of 8.6 is associated with this item; the vector string is pending confirmation from an authoritative source (NVD or vendor advisory). No NVD entry, CISA KEV listing, EPSS score, or vendor-issued patch advisory was present in the source dataset. Affected version range is unconfirmed. Confidence in CVE existence and SSRF/CWE-918 technical mapping is assessed as medium,

based on multiple corroborating secondary sources in the absence of an NVD or vendor primary confirmation.

## Action Checklist

1. Step 1: Containment. Identify all self-hosted typebot deployments in your environment. If the service is internet-facing, restrict inbound access to trusted IP ranges via firewall or WAF rules until a vendor advisory or patch is available. Block outbound HTTP/HTTPS requests from the typebot application server to internal RFC 1918 address space and cloud metadata endpoints (e.g., 169.254.169.254) at the network perimeter. Per NIST SC-7 (Boundary Protection), enforce egress filtering on managed interfaces.
2. Step 2: Detection. Query application and proxy logs for outbound HTTP requests originating from the typebot server process targeting internal IP ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) or known metadata endpoints. Review web server access logs (NIST AU-2, Event Logging) for anomalous server-initiated request patterns. Monitor for DNS lookups and outbound connections to unexpected external hosts originating from the typebot process. Apply proxy-based web server access mediation (e.g., WAF or egress proxy) to intercept and inspect server-side outbound requests.
3. Step 3: Eradication. No vendor-confirmed patch or remediation advisory is available in the source dataset as of this writing. Monitor the official Typebot repository (https://github.com/baptisteArno/typebot.io) for security advisories and apply any issued patch or version upgrade immediately. Until a patch is available, disable or sandbox HTTP request and script execution features within typebot if operationally feasible. Per CIS 7.2 (Establish and Maintain a Remediation Process), document this gap and assign a remediation owner with a defined review cadence.
4. Step 4: Recovery. After applying any vendor-issued patch or configuration mitigation, validate that outbound server-side HTTP requests to internal address space are blocked via firewall rule testing. Re-enable typebot services incrementally and monitor egress traffic patterns for 72 hours post-remediation. Confirm logging is intact per NIST AU-12 (Audit Record Generation) and CIS 8.2 (Collect Audit Logs) before returning the service to full production traffic.
5. Step 5: Post-Incident. Assess whether outbound egress filtering was applied to application servers prior to this disclosure; if not, close that control gap. Review whether cloud metadata endpoint access (IMDSv2 enforcement on AWS, equivalent on Azure/GCP) is enforced for all hosts running third-party web applications. Document findings against NIST SC-7 (Boundary Protection) and update the vulnerability management process per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to include SSRF-class risks in application server hardening standards.

## Detection Guidance

Monitor outbound HTTP and HTTPS connections from the typebot application server process. Key patterns to hunt: requests targeting 169.254.169.254 or 169.254.170.2 (cloud metadata), RFC 1918 address space, localhost (127.0.0.1), or internal hostname patterns not consistent with normal typebot operation. In proxy or WAF logs, look for server-originated GET/POST requests where the destination URL is user-controlled input passed to an HTTP request node. SSRF exploitation may also appear as unusual DNS resolution requests from the application server to internal domain names. If available, correlate application-layer logs from the typebot process with network flow data to identify lateral movement attempts following metadata credential theft. Apply proxy-based web server access mediation (e.g., WAF or egress proxy) to enforce allowlist-based egress from the application tier. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for structured log

analysis cadence.

## Framework Mappings

### MITRE-ATTACK

- **T1090.002** — External Proxy
- **T1071.001** — Web Protocols

### OWASP-TOP10-2021

- **A10:2021** — Server-Side Request Forgery (SSRF)

### NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-10** — Information Input Validation

### CIS-V8

- **13.4** — Perform Traffic Filtering Between Network Segments

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1090.002 | External Proxy | Command-And-Control |
| T1071.001 | Web Protocols | Command-And-Control |

## Sources

| Source | URL | Tier |
|---|---|---|
| **CVE-2026-48764 - CVE Details, Severity, and Analysis \| Strobes VI** | https://vi.strobes.co/cve/CVE-2026-48764 | T3 |
| **CVE-2026-48764 - TypeBot has SSRF in HTTP request and script ...** | https://cvefeed.io/vuln/detail/CVE-2026-48764 | T3 |
| **CVE-2026-48764: CWE-918: Server-Side Request Forgery (SSRF ...** | https://radar.offseq.com/threat/cve-2026-48764-cwe-918-server-side-... | T3 |

| Source | URL | Tier |
|---|---|---|
| NVD | https://nvd.nist.gov/vuln/detail/CVE-2026-48764 | T1 |



Generated 2026-06-18 17:48 UTC by TJS Security Command Center