INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:21 UTC

CVE-2026-48768: Path Traversal Vulnerability in baptisteArno typebot.io

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0330
Type	CVE Vulnerability
CVE ID	CVE-2026-48768
Severity	HIGH
CVSS Base Score	7.5
Affected Products	baptisteArno typebot.io (specific version range unconfirmed, source: gemini, secondary tier)
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

A path traversal vulnerability (CVE-2026-48768, CWE-22) has been reported in baptisteArno typebot.io, an open-source chatbot builder used in web application workflows. If exploited, an attacker could read or manipulate files outside the application's intended directory, potentially exposing configuration files, credentials, or sensitive user data. Confidence in full technical details is low pending primary-source confirmation; organizations running typebot.io should treat this as a credible risk and assess exposure while awaiting NVD publication.

Technical Analysis

CVE-2026-48768 describes a path traversal flaw (CWE-22) in baptisteArno typebot.io. Path traversal vulnerabilities occur when user-supplied input is used to construct file paths without adequate sanitization, allowing sequences such as '../' to escape the intended directory. This maps to MITRE ATT&CK T1083 (File and Directory Discovery), suggesting the primary attacker objective is unauthorized file read, though write-path exploitation enabling arbitrary file manipulation has also been reported in the description. Affected version range is unconfirmed. No CVSS vector string is available in source data; the qualitative rating is High with a reported CVSS base score of 7.5. No NVD entry, CISA KEV listing, or vendor advisory was confirmed at analysis time. Note: identifier confusion has been observed, one secondary source (SentinelOne) addresses CVE-2026-8768 (Vercel AI SSRF), a distinct vulnerability; ensure triage references CVE-2026-48768 only. EPSS data was not available. Primary-source verification is required before treating any specific technical details as confirmed.

Action Checklist

1. Step 1: Containment, Identify all instances of baptisteArno typebot.io running in your environment (self-hosted deployments and any integrated pipeline components). Restrict inbound access to typebot.io services to known-good IP ranges or place them behind a WAF with path traversal ruleset enabled. If internet-facing, consider temporary takedown of the affected service until patch status is confirmed. Reference CIS 4.1-4.2 (Firewall Standards and Rules).
2. Step 2: Detection, Review web server and application logs for requests containing path traversal sequences: '../', '..%2F', '..%5C', and URL-encoded variants. Query for HTTP 200 responses to requests referencing system file paths ('/etc/passwd', '.env', 'config.json', 'credentials'). Enable or verify logging per NIST AU-2 (Event Logging) and AU-3 (Content of Audit Records). Monitor application directories for unexpected read or modification events. No confirmed IOC patterns or specific event IDs are available from source data at this time.
3. Step 3: Eradication, Monitor the official baptisteArno/typebot GitHub repository and typebot.io release channels for a patched version. Apply the vendor-issued update as soon as available. Until a patch is confirmed, implement server-side input validation to reject path traversal sequences at the application or reverse proxy layer. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management). Do not rely solely on WAF filtering as a permanent remediation.
4. Step 4: Recovery, After applying the patch or validated mitigation, verify that no unauthorized files were accessed or modified during the exposure window. Audit files in the typebot.io working directory and parent directories for unexpected access timestamps. Rotate any credentials, API keys, or secrets stored in files accessible to the application. Re-enable full service access only after confirming clean state. Continue monitoring per NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident, Review whether secrets and configuration files are stored outside the web root and inaccessible to the application user account (NIST AC-6, Least Privilege). Assess whether CIS 7.1 (Establish and Maintain a Vulnerability Management Process) includes coverage for open-source and third-party chatbot/workflow components. Document this exposure in your risk register pending NVD confirmation of full technical details.

Detection Guidance

Query web application and reverse proxy logs for path traversal patterns in request URIs: sequences including '../', '..%2F', '..%5C', '%2e%2e%2f', and double-encoded variants. Filter for HTTP 200 or 206 responses to requests referencing sensitive filenames such as '.env', 'config', 'passwd', 'shadow', or key/certificate file extensions (.pem, .key, .p12). Alert on any successful read of files outside the typebot.io application root directory. Configure file integrity monitoring on the typebot.io working directory and parent paths to detect unexpected access. No confirmed exploit-specific IOC patterns, payload hashes, or source IPs are available from the source data at this time. Detection specificity will improve once a vendor advisory or NVD entry is published.

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
CVE-2026-48768 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-48768	T1
CVE-2026-48768 - CVE Details, Severity, and Analysis | Strobes VI	https://strobes.co/vi/cve/CVE-2026-48768/	T3
CVE-2026-8768: Vercel AI SSRF Vulnerability - SentinelOne	https://www.sentinelone.com/vulnerability-database/cve-2026-8768/	T3
CVE-2026-48768 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-48768	T3
[Threat Intel] May 22, 2026 Vulnerability Intelligence Briefing - Reddit	https://www.reddit.com/r/Network/comments/1tnvomo/threat_intel_may_...	T3

Generated 2026-06-18 17:21 UTC by TJS Security Command Center