INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-18 17:20 UTC

CVE-2026-11395: Server-Side Request Forgery in CF7 to Webhook Plugin for WordPress

CVE VULNERABILITY | **HIGH** | CVSS 8.6

SCC Item ID	SCC-CVE-2026-0329
Type	CVE Vulnerability
CVE ID	CVE-2026-11395
Severity	HIGH
CVSS Base Score	8.6
Affected Products	CF7 to Webhook plugin for WordPress, all versions up to and including 5.0.0
Published	2026-06-18
Discovery Source	Gemini

Executive Summary

A server-side request forgery vulnerability in the CF7 to Webhook WordPress plugin (versions up to and including 5.0.0) allows unauthenticated attackers to direct the vulnerable web server to make arbitrary requests against internal network resources. Exploitation requires a specific administrator-configured webhook condition, reducing but not eliminating real-world risk. Organizations running this plugin on internet-facing WordPress sites should assess their webhook configurations and apply remediation immediately.

Technical Analysis

CVE-2026-11395 is a server-side request forgery (SSRF) vulnerability, classified under CWE-918, affecting the CF7 to Webhook plugin for WordPress in all versions up to and including 5.0.0. The vulnerability is exploitable without authentication when two preconditions are met: an administrator has configured a webhook URL that embeds a Contact Form 7 field placeholder within the host segment, and the affected form is publicly accessible. When those conditions exist, an unauthenticated attacker can manipulate form field values to redirect outbound HTTP requests from the WordPress server to arbitrary internal network destinations, potentially reaching internal APIs, cloud metadata services (e.g., AWS IMDS at 169.254.169.254), or other services not exposed externally. CVSS base score is 8.6 (vector pending NVD publication). MITRE ATT&CK techniques T1090 (Proxy) and T1083 (File and Directory Discovery) are associated with post-exploitation behavior enabled by SSRF primitives. No CISA KEV listing or active exploitation has been recorded in the provided data. Patch status: update beyond version 5.0.0 per vendor guidance.

Action Checklist

1. Step 1: Containment. Immediately audit all CF7 to Webhook plugin configurations across WordPress instances. Identify any webhook URLs where a Contact Form 7 field placeholder (e.g., [field-name]) appears within the host or hostname segment of the URL. If found, remove or reconfigure that webhook URL to use a hardcoded, trusted host. Disable the plugin on publicly accessible forms until configuration is verified safe. (NIST AC-4: Information Flow Enforcement)
2. Step 2: Detection. Query web server and application logs for outbound HTTP requests originating from the WordPress process that target RFC-1918 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), loopback (127.0.0.1), or cloud metadata endpoints (169.254.169.254). Review Contact Form 7 submission logs for form field values containing IP addresses, internal hostnames, or URL-formatted strings in fields that feed webhook host segments. Review WAF logs for anomalous POST requests to CF7-enabled form endpoints. (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs)
3. Step 3: Eradication. Update the CF7 to Webhook plugin to a version beyond 5.0.0 that addresses CVE-2026-11395 per the plugin vendor's release notes. Confirm the updated version validates or sanitizes the host segment of webhook URLs against user-supplied input. If no patched version is yet available, disable the plugin entirely until a fix is released. Implement server-side egress filtering to block outbound requests from the web server to internal network ranges and cloud metadata IPs. (NIST SI-4; CIS 7.3: Perform Automated Operating System Patch Management; CIS 7.4: Perform Automated Application Patch Management; D3-UAP: User Account Permissions)
4. Step 4: Recovery. After applying the plugin update, re-enable only forms with webhook configurations verified to use hardcoded, external, trusted URLs in the host segment. Run a targeted SSRF probe (in a controlled test environment or via your vulnerability management program) against the updated plugin to confirm the injection point is closed. Monitor egress traffic and application logs for 72 hours post-remediation for any residual anomalous outbound requests. (NIST AU-6; CIS 7.1: Establish and Maintain a Vulnerability Management Process)
5. Step 5: Post-Incident. Document the webhook configuration pattern that created exposure and add it to your WordPress hardening baseline. Establish a recurring review process for CF7 and similar plugin webhook/callback configurations that accept dynamic URL components. Evaluate whether egress firewall rules for web application servers adequately restrict access to internal network ranges and metadata endpoints as a defense-in-depth layer. Map this gap to NIST AC-4 (Information Flow Enforcement) in your risk register. (CIS 4.4: Implement and Manage a Firewall on Servers; D3-PBWSAM: Proxy-based Web Server Access Mediation)

Detection Guidance

Focus detection on two signals: anomalous outbound HTTP requests from the WordPress server process, and suspicious form field values in CF7 submissions. In web server or WAF logs, flag POST requests to CF7 form endpoints where the referencing webhook subsequently generates an outbound connection to an RFC-1918 address, loopback, or 169.254.169.254 (cloud metadata). In application logs, search for CF7 field submission values matching patterns: IPv4 addresses, internal hostnames, or URL-formatted strings (regex: ^(https?://)?(10\.|172\.(1[6-9]|2[0-9]|3[01])\.|192\.168\.|127\.|169\.254\.)). If your WordPress host runs in a cloud environment, alert on any process-level outbound connection to 169.254.169.254 that is not expected from your application. MITRE T1090 (Proxy) activity may surface as the WordPress server appearing as an origin for requests to internal services in network flow logs. No confirmed IOCs are available in the source data; detections should be behavior-based. (NIST AU-6; CIS 8.2)

Framework Mappings

MITRE-ATTACK

- **T1090** — Proxy
- **T1083** — File and Directory Discovery

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090	Proxy	Command-And-Control
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
April 2026 CVE Landscape - Recorded Future	https://www.recordedfuture.com/blog/april-cve-landscape	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-11395	T1

Generated 2026-06-18 17:20 UTC by TJS Security Command Center