Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Is Your Spring Config Server an Open Door? CVE-2026-40982 Says Yes

Date of Publication	Admiralty Code	TA Number
May 08, 2026	A1	TA2026123

Summary

First Seen: May 06, 2026
Affected Products: Spring Cloud Config Server
Impact: A critical directory traversal vulnerability tracked as CVE-2026-40982 has been disclosed in the spring-cloud-config-server module of VMware's Spring Cloud Config project, an open-source distributed configuration framework widely deployed in microservice and cloud-native architectures. The vulnerability allows an unauthenticated, remote attacker to retrieve arbitrary files from any host running an affected version of Spring Cloud Config Server, exposing the contents of operating system files, application source, deployment manifests, and any secrets, tokens, certificates, or credentials accessible to the service account.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-40982	VMware Spring Cloud Config Server Path Traversal Vulnerability	VMware Spring Cloud Config Server	✗	✗	✓

Vulnerability Details

#1

A critical directory traversal vulnerability tracked as CVE-2026-40982 has been disclosed in the spring-cloud-config-server module of VMware's Spring Cloud Config project, an open-source distributed configuration framework widely deployed in microservice and cloud-native architectures. The flaw arises because the module is designed to serve arbitrary text and binary files, and an unauthenticated remote attacker can submit a specially crafted URL request that escapes the intended serving directory and reads files elsewhere on the host filesystem. This vulnerability is rated Critical by the vendor and was disclosed on May 06, 2026.

#2

Because Spring Cloud Config Server is purpose-built to centralize configuration for downstream microservices, file disclosure on the configuration plane often translates directly to lateral compromise of every consuming service, environment-specific credentials, and backend infrastructure. The combination of network-reachable attack surface, no authentication requirement, low complexity, and high confidentiality and integrity impact creates substantial business risk for any organization running affected branches in production, staging, or DevOps tooling, including downstream supply-chain risk to applications that trust configuration retrieved from these servers.

#3

The root cause lies in the spring-cloud-config-server module's intended functionality of serving arbitrary text and binary files to client applications that retrieve their configuration from the central server. The serving logic does not adequately constrain the requested path to the configured base directory, and as a result, an attacker who supplies a specially crafted URL containing traversal sequences can escape the intended directory boundary and read files located elsewhere on the host filesystem. Because the module exposes its endpoints over HTTP and does not require authentication for the affected behavior, the attack vector is fully network-based, with no privileges and no user interaction needed. The scope of impact spans every actively maintained branch of Spring Cloud Config.

#4

The vulnerability was independently discovered and responsibly disclosed by Rashmi Singh (rash18mi) from Hive Pro, Swapnil Paliwal, and the security team at AxiomCode using the AxiomEngine, August829, and Yu Bao. It was not exploited as a zero-day prior to disclosure. As of the publication of this advisory, the available sources report no confirmed in-the-wild exploitation. Given the severity of the flaw, the trivial attack complexity, and the typical sensitivity of data stored on configuration servers, however, the time-to-exploit window after public disclosure is expected to be short, and defenders should treat the patch as urgent.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-40982	VMware Spring Cloud Config Server 3.1.0 through 3.1.13; 4.1.0 through 4.1.9; 4.2.0 through 4.2.6; 4.3.0 through 4.3.2; 5.0.0 through 5.0.2; and older unsupported versions	cpe:2.3:a:vmware:spring_cloud_config:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Apply the Vendor Patch Without Delay: Upgrade every Spring Cloud Config Server instance to the corresponding fixed release for its branch - 3.1.14, 4.1.10, 4.2.7, 4.3.3, or 5.0.3. The 4.3.3 and 5.0.3 fixes are available through Open Source Software channels, while fixes for the 3.1.x, 4.1.x, and 4.2.x branches require an active VMware/Broadcom Enterprise Support subscription. Inventory all running config-server pods, JARs, and embedded library versions before patching, and validate the upgrade in a staging environment before production rollout.

Restrict Network Exposure of the Config Server: Confirm that the config-server endpoints are not directly reachable from the public internet. Place the service behind an authenticated ingress, an internal service mesh, or a private network segment, and restrict source IP access to known service consumers and operations tooling. Reducing attack surface buys time when a fast-moving vulnerability like this one is disclosed and shrinks the population of opportunistically exploitable hosts.

Hunt for Indicators of Prior Exploitation: Review reverse proxy, ingress controller, and application access logs for HTTP requests to config-server endpoints that contain encoded or unencoded path traversal sequences (for example, occurrences of `../`, `..%2f`, `%2e%2e/`, or unusually deep relative paths) preceding the disclosure date. Correlate any such activity with downstream secret access, anomalous service-to-service authentication, or unexpected outbound connections from the config-server host, and treat hits as potential pre-disclosure reconnaissance or exploitation attempts.

Rotate Secrets Reachable by the Config Server: Because a successful path traversal yields arbitrary file read on the configuration plane, assume that any credential, API key, certificate, signing key, or backend token reachable on disk by the config-server service account may have been exposed if the host was internet-facing. Rotate these secrets, invalidate cached tokens, and re-issue certificates as part of the post-patch hygiene cycle, prioritizing secrets used to access production data stores and identity providers.

Run the Service with Least Privilege: Operate Spring Cloud Config Server under a dedicated, low-privilege service account whose filesystem access is restricted to the configuration repository and required runtime files. Remove read access to OS-level secrets, SSH keys, environment files, and unrelated application data wherever feasible. Combined with container/pod-level read-only filesystem mounts, this control materially reduces the blast radius of any future arbitrary-file-read class vulnerability in this or adjacent components.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
Initial Access	T1190: Exploit Public-Facing Application	
Discovery	T1083: File and Directory Discovery	
Collection	T1005: Data from Local System	

Patch Link

https://github.com/spring-cloud/spring-cloud-config/releases

References

https://spring.io/security/cve-2026-40982

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 08, 2026 • 2:00 AM

More at www.hivepro.com