

CVE-2020-5410

VMware Tanzu Spring Cloud Config Directory Traversal Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.

EVRS 83/₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.956 99.87th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.956 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.springframework.cloud:spring-cloud-config-server	2.1.0, < 2.1.9	2.1.9	GitHub
org.springframework.cloud:spring-cloud-config-server	2.2.0, < 2.2.3	2.2.3	GitHub
spring cloud config	≥ 2.1.0 < 2.1.9 ≥ 2.2.0 < 2.2.3	2.1.9 · 2.2.3	NVD

Sources

Vendor guidance tanzu.vmware.com/security/cve-2020-5410

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-0451

NVD nvd.nist.gov/vuln/detail/CVE-2020-5410

GitHub advisory github.com/advisories/GHSA-32xf-jwmv-9hf3

Current data evulnable.com/vulnerability-management/cve/CVE-2020-5410

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.