

CVE-2022-22963

VMware Tanzu Spring Cloud Function Remote Code Execution Vulnerability

Exigent
CISA KEV since Aug 25, 2022
Actively exploited
Public exploit module (Metasploit)

In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Sep 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	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions · 20 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.springframework.cloud:spring-cloud-function-context	3.2.0, < 3.2.3	3.2.3	GitHub
org.springframework.cloud:spring-cloud-function-context	3.1.7	3.1.7	GitHub
spring cloud function	≤ 3.1.6 ≥ 3.2.0 ≤ 3.2.2	after 3.1.6 · after 3.2.2	NVD
banking branch	14.5	no fixed version listed	NVD
banking cash management	14.5	no fixed version listed	NVD
banking corporate lending process management	14.5	no fixed version listed	NVD
banking credit facilities process management	14.5	no fixed version listed	NVD
banking electronic data exchange for corporates	14.5	no fixed version listed	NVD
banking liquidity management	14.2 14.5	no fixed version listed	NVD
banking origination	14.5	no fixed version listed	NVD



Sources

Vendor guidance	oracle.com/security-alerts/cpuapr2022.html	Additional guidance	tanzu.vmware.com/security/cve-2022-22963
	NVD nvd.nist.gov/vuln/detail/CVE-2022-22963		CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-6v73-fg6-w5j7	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-1654
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-22963		

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