

CVE-2020-10221

rConfig OS Command Injection Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

lib/ajaxHandlers/ajaxAddTemplate.php in rConfig through 3.94 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the fileName POST parameter.

EVRS 80 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.771 99.55th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.771 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
rconfig	≤ 3.9.4	after 3.9.4	NVD

Sources

Vendor guidance	cwe.mitre.org/data/definitions/78.html	Additional guidance	engindemirbilek.github.io/rconfig-3.93-rce
Additional guidance	github.com/EnginDemirbilek/EnginDemirbilek.github.io/blob/master/rconfig-3.93-rce.html	NVD	nvd.nist.gov/vuln/detail/CVE-2020-10221
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-2679
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-10221		

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