

CVE-2020-12641

Roundcube Webmail Remote Code Execution Vulnerability

CISA KEV since Jun 22, 2023

Actively exploited

rcube_image.php in Roundcube Webmail before 1.4.4 allows attackers to execute arbitrary code via shell metacharacters in a configuration setting for im_convert_path or im_identify_path.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.845 99.7th percentile · FIRST	CISA DEADLINE Jul 13, 2023 KEV since 2023 · 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	0.845 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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
webmail	$\geq 1.2.0 < 1.2.10$ $\geq 1.3.0 < 1.3.11$ $\geq 1.4.0 < 1.4.4$	no fixed version listed	NVD
backports sle	15.0	no fixed version listed	NVD
leap	15.1 15.2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/roundcube/roundcubemail/commit/fcfb099477f353373c34c8a65c9035b06b364db3	Additional guidance	roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10
NVD	nvd.nist.gov/vuln/detail/CVE-2020-12641	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-4942	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-12641

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