

CVE-2020-35730

Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability

CISA KEV since Jun 22, 2023

Actively exploited

An XSS issue was discovered in Roundcube Webmail before 1.2.13, 1.3.x before 1.3.16, and 1.4.x before 1.4.10. The attacker can send a plain text e-mail message, with JavaScript in a link reference element that is mishandled by linkref_addindex in rcube_string_replacer.php.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 6.1 Medium · NVD	EPSS 0.329 98.4th 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	0.329 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.1	☐ 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	< 1.2.13 ≥ 1.3.0 < 1.3.16 ≥ 1.4 < 1.4.10	no fixed version listed	NVD
fedora	32 33	no fixed version listed	NVD
debian linux	9.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/roundcube/roundcubemail/compare/1.4.9...1.4.10	Additional guidance	lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HMLIZWKMTRCLU7KZLEQHELS4INXJ7X5Q/nvd.nist.gov/vuln/detail/CVE-2020-35730
roundcube.net	roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13	NVD	
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-23386
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-35730		

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