

CVE-2023-5631

Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability

CISA KEV since Oct 26, 2023

Actively exploited

Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.4 Medium · NVD	EPSS 0.769 99.55th percentile · FIRST	CISA DEADLINE Nov 16, 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	0.769 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
webmail	< 1.4.15 ≥ 1.5.0 < 1.5.5 ≥ 1.6.0 < 1.6.4	no fixed version listed	NVD
debian linux	10.0 11.0 12.0	no fixed version listed	NVD
fedora	39	no fixed version listed	NVD

Sources

Vendor guidance	bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079	roundcube.net	roundcube.net/news/2023/10/16/security-update-1.6.4-released , https://roundcube.net/news/2023/10/16/security-updates-1.5.5-and-1.4.15
NVD	nvd.nist.gov/vuln/detail/CVE-2023-5631	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-57924	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-5631

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