

CVE-2017-16651

Roundcube Webmail File Disclosure Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Roundcube Webmail before 1.1.10, 1.2.x before 1.2.7, and 1.3.x before 1.3.3 allows unauthorized access to arbitrary files on the host's filesystem, including configuration files, as exploited in the wild in November 2017. The attacker must be able to authenticate at the target system with a valid username/password as the attack requires an active session. The issue is related to file-based attachment plugins and `_task=settings&_action=upload-display&_from=timezone` requests.

EVRS 75/100 Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.457 98.8th 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	0.457 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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	≤ 1.1.9 1.2.0 1.2.1 1.2.2 1.2.3 1.2.4 1.2.5 1.2.6 1.3.0 1.3.1 1.3.2	no fixed version listed	NVD
debian linux	7.0 9.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/roundcube/roundcubemail/issues/6026

NVD nvd.nist.gov/vuln/detail/CVE-2017-16651

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-7838

Additional guidance roundcube.net/news/2017/11/08/security-updates-1.3.3-1.2.7-and-1.1.10

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2017-16651

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