AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi të Shfrytëzuara Aktivisht në Roundcube Webmail

Data: 23/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 2
Referenca 2

Përmbledhje Ekzekutive

Dy dobësi të rëndësishme sigurie janë identifikuar dhe publikuar në Roundcube Webmail. Dobësia e parë (**CVE-2025-49113**) vlerësohet **kritike (CVSS 9.9)** dhe lejon ekzekutim kodi nga distanca të autentikuar përmes **PHP Object Deserialization**. Dobësia e dytë (**CVE-2025-68461**) vlerësohet **e lartë (CVSS 7.2)** dhe mundëson **Cross-Site Scripting (XSS)** përmes përmbajtjes SVG keqdashëse.

Të dyja dobësitë janë adresuar në publikimet e sigurisë **1.6.12** dhe **1.5.12**, të publikuara më **13 Dhjetor 2025**. Të dy CVE-të janë të listuara si **Known Exploited Vulnerabilities (KEV)**, që do të thotë se duhet të supozohet shfrytëzim aktiv në terren.

Informacione Teknike

Detaje të Dobësive:

1. CVE-2025-49113 — Ekzekutim Kodi nga Distanca përmes PHP Object Deserialization

- CVE ID: CVE-2025-49113
- CVSS Score: 9.9 — kritike
- CWE: CWE-502 — Deserialization i të Dhënave të Pabesueshme
- Versionet e prekura:
  - Roundcube Webmail versionet 0 deri para 1.5.10
  - Roundcube Webmail versionet 1.6.0 deri para 1.6.11
- Rregulluar në: 1.5.10 / 1.6.11 (dhe më pas: 1.5.12 / 1.6.12)

2. CVE-2025-68461 — Cross-Site Scripting (XSS) përmes SVG Animate Tag

- CVE ID: CVE-2025-68461
- CVSS Score: 7.2 — e lartë
- CWE: CWE-79 — Neutralizim i pasaktë i input-it gjatë gjenerimit të faqeve web (XSS)
- Versionet e prekura:
  - Roundcube Webmail versionet 0 deri para 1.5.12
  - Roundcube Webmail versionet 1.6.0 deri para 1.6.12
- Rregulluar në: 1.5.12 / 1.6.12

Rekomandime

Rekomandohet të përditësoni menjëherë të gjitha instancat Roundcube Webmail në versionin e rregulluar ose në versionin më të fundit.

Referenca

https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12