Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0181

Kwetsbaarheid verholpen in Roundcube Webmail

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 05-06-2025
Revisie: 1.0.2

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 2

Het NCSC heeft signalen ontvangen dat exploitcode in omloop is waarmee de kwetsbaarheid kan worden misbruikt. De inschaling van dit beveiligingsadvies is daarom veranderd naar HIGH/HIGH. Het NCSC adviseert organisaties met klem om de door Roundcube beschikbaar gestelde beveiligingsupdates te installeren.

Feiten

Roundcube heeft een kwetsbaarheid verholpen in Roundcube Webmail (specifiek versies vóór 1.5.10 en 1.6.x vóór 1.6.11).

Duiding

Een geauthenticeerde kwaadwillende kan de kwetsbaarheid misbruiken voor het uitvoeren van willekeurige code. Hiertoe dient de kwaadwillende een malafide HTTP-request naar de Roundcube-applicatie te versturen. De kwetsbaarheid wordt veroorzaakt door inadequate validatie van userinput in de _from-parameter.

Het NCSC heeft signalen ontvangen dat exploitcode in omloop is waarmee de kwetsbaarheid kan worden misbruikt. Dit verhoogt het risico op misbruik aanzienlijk.

Oplossingen

Roundcube heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Het NCSC adviseert organisaties met klem om de door Roundcube beschikbaar gestelde beveiligingsupdates te installeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-49113	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-502	Deserialization of Untrusted Data

Getroffen producten

RoundCube
Webmail

Disclaimer