Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0242

Kwetsbaarheden verholpen in RoundCube Webmail

2024-06-07 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

RoundCube heeft kwetsbaarheden verholpen in RoundCube Webmail.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Cross-Site-Scripting-aanval uit te voeren. Een dergelijke aanval kan leiden tot uitvoer van willekeurige code in de browser van het slachtoffer en mogelijk toegang tot gevoelige gegevens in de context van de browser van het slachtoffer. Omdat het hier een webmail-toepassing betreft kan de kwaadwillende hiermee toegang krijgen tot gevoelige e-mails.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide link te openen.

Oplossingen

RoundCube heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Webmail 1.5.7 en 1.6.7. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/roundcube/roundcubemail/releases/tag/1.5.7
- https://github.com/roundcube/roundcubemail/releases/tag/1.6.7