



# CVE-2020-12641

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-12641
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-04 15:15:00 UTC
<b>Updated</b>	2022-04-29 13:24:00 UTC
<b>Description</b>	rcube_image.php in Roundcube Webmail before 1.4.4 allows attackers to execute arbitrary code via shell metacharacters in

## Risk And Classification

**EPSS:** 0.931330000 probability, percentile 0.997930000 (date 2026-04-02)

**CISA KEV:** Listed on 2023-06-22; due 2023-07-13; ransomware use Unknown

**Problem Types:** CWE-78

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Roundcube
<b>Product</b>	Roundcube Webmail
<b>Name</b>	Roundcube Webmail Remote Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10;">https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10;</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2020-12641">https://nvd.nist.gov/vuln/detail/CVE-2020-12641</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openseuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Application	<a href="#">Openseuse</a>	<a href="#">Backports Sle</a>	15.0	sp2	All	All
Operating System	<a href="#">Openseuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Openseuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Application	<a href="#">Roundcube</a>	<a href="#">Webmail</a>	All	All	All	All
Application	<a href="#">Roundcube</a>	<a href="#">Webmail</a>	All	All	All	All

## References

## REFERENCES

Reference	Source	Link
Release Roundcube Webmail 1.4.4 · roundcube/roundcubemail · GitHub	MISC	<a href="#">github.c</a>
Disclosures/CVE-2020-12641-Command Injection-Roundcube at master · DrunkenShells/Disclosures · GitHub	MISC	<a href="#">github.c</a>
Comparing 1.4.3...1.4.4 · roundcube/roundcubemail · GitHub	MISC	<a href="#">github.c</a>
Roundcube: Multiple vulnerabilities (GLSA 202007-41) — Gentoo security	GENTOO	<a href="#">security</a>
[security-announce] openSUSE-SU-2020:1516-1: moderate: Security update f	SUSE	<a href="#">lists.ope</a>
Fix remote code execution via crafted 'im_convert_path' or 'im_identi...' · roundcube/roundcubemail@fcfb099 · GitHub	MISC	<a href="#">github.c</a>
Security updates 1.4.4, 1.3.11 and 1.2.10 released	MISC	<a href="#">roundcu</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="#">www.cis</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)