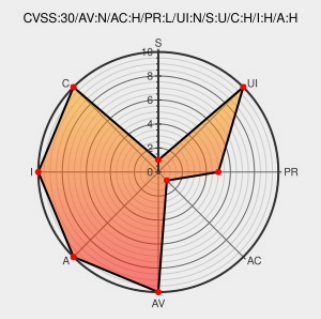
CVE-2015-8770

Published on: 01/29/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8770

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Roundcube Webmail from Roundcube contain the following vulnerability:

Directory traversal vulnerability in the set_skin function in program/include/rcmail_output_html.php in Roundcube before 1.0.8 and 1.1.x before 1.1.4 allows remote authenticated users with certain permissions to read arbitrary files or possibly execute arbitrary code via a .. (dot dot) in the _skin parameter to index.php.

CVE-2015-8770 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Roundcube Webmail 1.1.3 - Directory Traversal	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39245

[security-announce] openSUSE-SU-2016:0213-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0213
Roundcube 1.1.3 Path Traversal ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135274/Roundcube-1.1.3-Path-Traversal.html
File Not Found	Exploit www.htbridge.com text/html Inactive Link Not Archived	MISC www.htbridge.com/advisory/HTB23283
[security-announce] openSUSE-SU-2016:0214-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0214
Roundcube: Multiple Vulnerabilities (GLSA 201603-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201603-03
404 Not Found	trac.roundcube.net text/html Inactive Link Not Archived	CONFIRM trac.roundcube.net/changeset/10e5192a2b/github
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160113 Remote Code Execution in Roundcube
[security-announce] openSUSE-SU-2016:0210-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0210
#1490620 (Roundcube Security Vulnerability Notification) – Roundcube Webmail	trac.roundcube.net text/html	CONFIRM trac.roundcube.net/ticket/1490620
Updates 1.1.4 and 1.0.8 released	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM roundcube.net/news/2015/12/26/updates-1.1.4-and-1.0.8-released/
Debian -- Security Information -- DSA-3541-1 roundcube	www.debian.org Depreciated Link text/html	DEBIAN DSA-3541

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Roundcube	Roundcube Webmail	1.1.0	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.1	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.2	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.3	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.0	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.1	All	All	All

Application	Roundcube	Roundcube Webmail	1.1.2	All	All	All
Application	Roundcube	Roundcube Webmail	1.1.3	All	All	All
Application	Roundcube	Roundcube Webmail	All	All	All	All

cpe:2.3:a:roundcube:roundcube_webmail:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:roundcube_webmail:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→