

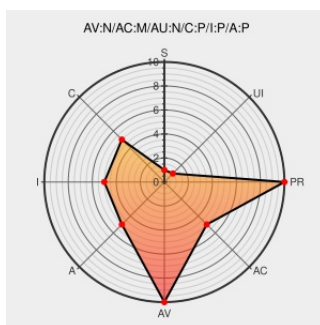


CVE-2014-0791

Published on: 01/03/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:56 PM UTC

CVE-2014-0791

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Freerdp](#) from [Freerdp](#) contain the following vulnerability:

Integer overflow in the `license_read_scope_list` function in `libfreerdp/core/license.c` in FreeRDP through 1.0.2 allows remote RDP servers to cause a denial of service (application crash) or possibly have unspecified other impact via a large `ScopeCount` value in a `Scope List` in a `Server License Request` packet.

CVE-2014-0791 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

openSUSE-SU-2016:2400-1:
moderate: Security update for freerdp

lists.opensuse.org
text/html

[SUSE openSUSE-SU-2016:2400](#)

Support / Security / Advisories //
MDVSA-2015:171 | Mandriva

www.mandriva.com
text/html

[MANDRIVA MDVSA-2015:171](#)

Fix possible integer overflow in
`license_read_scope_list()` by
sidhpurwala-huzaifa · Pull Request
#1649 · FreeRDP/FreeRDP · GitHub

github.com
text/html

[MISC github.com/FreeRDP/FreeRDP/pull/1649](https://github.com/FreeRDP/FreeRDP/pull/1649)

oss-security - CVE for freerdp int
overflow?

openwall.com
text/html

[MLIST \[oss-security\] 20140102 CVE for freerdp int overflow?](#)

Mageia Advisory: MGASA-2014-0287 -

advisories.mageia.org

[CONFIRM advisories.mageia.org/MGASA-2014-0287.html](https://advisories.mageia.org/MGASA-2014-0287.html)

Updated freerdp packages fix two vulnerabilities	text/html	
oss-security - Re: CVE for freerdp int overflow?	openwall.com text/html	 MLIST [oss-security] 20140103 Re: CVE for freerdp int overflow?
openSUSE-SU-2016:2402-1: moderate: Security update for freerdp	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:2402
[SECURITY] [DLA 2356-1] freerdp security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200829 [SECURITY] [DLA 2356-1] freerdp security update
998941 – (CVE-2014-0791) CVE-2014-0791 freerdp: integer overflow in heap allocation in license_read_scope_list()	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=998941
Fix possible integer overflow in license_read_scope_list() · sidhpurwala-huzaifa/FreeRDP@e274580 · GitHub	github.com text/html	 MISC github.com/sidhpurwala-huzaifa/FreeRDP/commit/e2745807c4c3e0a590c0f69a9b655dc74ebaa03e
openSUSE-SU-2014:0862-1: moderate: freerdp: Fixes for integer overflows	lists.opensuse.org text/html	 SUSE openSUSE-SU-2014:0862

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freerdp	Freerdp	1.0.0	All	All	All
Application	Freerdp	Freerdp	1.0.1	All	All	All
Application	Freerdp	Freerdp	1.0.2	All	All	All
Application	Freerdp	Freerdp	1.0.0	All	All	All
Application	Freerdp	Freerdp	1.0.1	All	All	All
Application	Freerdp	Freerdp	1.0.2	All	All	All
cpe:2.3:a:freerdp:freerdp:1.0.0:*:*:*:*:*:						
cpe:2.3:a:freerdp:freerdp:1.0.1:*:*:*:*:*:						
cpe:2.3:a:freerdp:freerdp:1.0.2:*:*:*:*:*:						
cpe:2.3:a:freerdp:freerdp:1.0.0:*:*:*:*:*:						
cpe:2.3:a:freerdp:freerdp:1.0.1:*:*:*:*:*:						
cpe:2.3:a:freerdp:freerdp:1.0.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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](#)