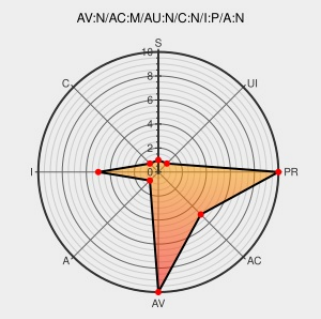
CVE-2011-2180

Published on: 06/29/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:21 PM UTC

CVE-2011-2180

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



Certain versions of Really Simple Chat from Reallysimplechat contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in dereferer.php in A Really Simple Chat (ARSC) 3.3-rc2 allows remote attackers to inject arbitrary web script or HTML via the arsc_link parameter.

CVE-2011-2180 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Re: CVE request: Multiple security vulnerabilities in ARSC Really Simple Chat	Exploit, www.openwall.com, text/html	MLIST [oss-security] 20110602 Re: CVE request: Multiple security vulnerabilities in ARSC Really Simple Chat
oss-security - CVE request: Multiple security vulnerabilities in ARSC Really Simple Chat	Exploit, www.openwall.com, text/html	MLIST [oss-security] 20110602 CVE request: Multiple security vulnerabilities in ARSC Really Simple Chat
High-Tech Bridge SA - Advisories - XSS in A Really Simple Chat (ARSC)	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.htbridge.ch/advisory/xss_in_a_really_simple_chat_arsc.html

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	Reallysimplechat	Really Simple Chat	3.3	rc2	All	All
Application	Reallysimplechat	Really Simple Chat	3.3	rc2	All	All

cpe:2.3:a:reallysimplechat:really_simple_chat:3.3:rc2:*:*:*:*:*:*:

cpe:2.3:a:reallysimplechat:really_simple_chat:3.3:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report