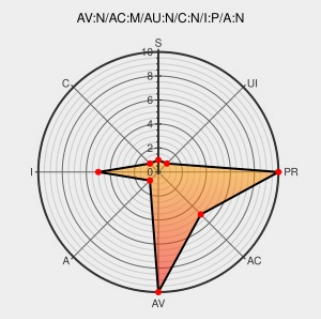
CVE-2009-3017

Published on: 08/31/2009 12:00:00 AM UTC

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

CVE-2009-3017

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



Certain versions of Orca Browser from Orcabrowser contain the following vulnerability:

Orca Browser 1.2 build 5 does not properly block data: URIs in Refresh and Location headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI, (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header, (3) injecting a Location header that contains JavaScript sequences in a data:text/html URI, or (4) entering a data:text/html URI with JavaScript sequences when specifying the content of a Location header; and does not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (5) injecting a Location HTTP response header or (6) specifying the content of a Location HTTP response header.

CVE-2009-3017 has been assigned by cve@mitre.org 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF orca-browser-data-xss(53002)
SecurityFocus	www.securityfocus.com	BUGTRAQ 20090828 Cross-Site Scripting vulnerability in

	text/html	Mozilla, Firefox, SeaMonkey, Orca Browser and Maxthon
Cross-Site Scripting attacks via redirectors - Websecurity - Веб безпека	Exploit websecurity.com.ua text/html	MISC websecurity.com.ua/3386/

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	Orcabrowser	Orca Browser	1.2	All	All	All
Application	Orcabrowser	Orca Browser	1.2	All	All	All

cpe:2.3:a:orcabrowser:orca_browser:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:orcabrowser:orca_browser:1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→