CVE-2012-1252

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-1252
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-04 15:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in RSSOwl before 2.1.1 allows remote attackers to inject arbitrary web script or HTM

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rssowl	Rssowl	2.0	All	All	All

Application	Rssowl	Rssowl	2.0	milestone5a	All	All
Application	Rssowl	Rssowl	2.0	milestone6	All	All
Application	Rssowl	Rssowl	2.0	milestone7	All	All
Application	Rssowl	Rssowl	2.0	milestone8	All	All
Application	Rssowl	Rssowl	2.0	milestone8a	All	All
Application	Rssowl	Rssowl	2.0	milestone9	All	All
Application	Rssowl	Rssowl	2.0	rc1	All	All
Application	Rssowl	Rssowl	2.0	rc2	All	All
Application	Rssowl	Rssowl	2.0	rc3	All	All
Application	Rssowl	Rssowl	2.0.1	All	All	All
Application	Rssowl	Rssowl	2.0.2	All	All	All
Application	Rssowl	Rssowl	2.0.3	All	All	All
Application	Rssowl	Rssowl	2.0.4	All	All	All
Application	Rssowl	Rssowl	2.0.5	All	All	All
Application	Rssowl	Rssowl	2.0.6	All	All	All
Application	Rssowl	Rssowl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
jvndb.jvn.jp/jvndb/JVNDB-2012-000048	af854a3a-2127-422b-91ae-364da2661108	jvndb.jvn.jp	
JVN#77947437: RSSOwl vulnerable to arbitrary script execution	af854a3a-2127-422b-91ae-364da2661108	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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