CVE-2012-4481

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2012-4481
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-02 14:55:00 UTC
Updated	2023-11-07 02:11:00 UTC
Description	The safe-level feature in Ruby 1.8.7 allows context-dependent attackers to modify strings via the NameError#to_s method v

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruby-lang	Ruby	1.8.7	All	All	All
Application	Ruby-lang	Ruby	1.8.7	All	All	All

References

Reference
Red Hat Customer Portal
Support / Security / Advisories / / MDVSA-2013:124 | Mandriva
Red Hat Customer Portal
oss-security - Re: CVE Request -- ruby (1.8.x with patched CVE-2011-1005): Incomplete fix for CVE-2011-1005 for NameError#to_s method v
Support/Advisories/MGASA-2012-0294 - Mageia wiki
Bug 863484 – CVE-2012-4481 ruby: Incomplete fix for CVE-2011-1005 for NameError#to_s method when used on objects
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
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 registred 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