



CVE-2009-0642

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-0642
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-20 06:47:00 UTC
Updated	2017-09-29 01:33:00 UTC
Description	ext/openssl/openssl_ocsp.c in Ruby 1.8 and 1.9 does not properly check the return value from the OCSP_basic_verify function

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruby-lang	Ruby	1.8	All	All	All
Application	Ruby-lang	Ruby	1.9	All	All	All
Application	Ruby-lang	Ruby	1.8	All	All	All
Application	Ruby-lang	Ruby	1.9	All	All	All

References

Reference
Ruby OCSP_basic_verify() Validation Flaw Lets Remote Users Conduct Certificate Spoofing Attacks - SecurityTracker
IBM X-Force Exchange
#513528 - ruby1.9: Not properly checking the return value of OCSP_basic_verify - Debian Bug report logs
Ruby 'OCSP_basic_verify()' X.509 Certificate Verification Vulnerability
Ruby "OCSP_basic_verify()" Certificate Validation Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com
Backport87 - Backport #1091: possible bad handling of return value of OCSP_basic_verify in ext/openssl/openssl_ocsp.c - Ruby Issue Tracking S
Support
Red Hat update for ruby - Secunia Advisories - Vulnerability Information - Secunia.com
Security Advisory SA35937 - Ubuntu update for Ruby - Secunia
Repository / Oval Repository

[USN-805-1: Ruby vulnerabilities | Ubuntu](#)

[Support / Security / Advisories / / MDVSA-2009:193 | Mandriva](#)

[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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)