



CVE-2014-2734

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

Summary

CVE	CVE-2014-2734
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-24 23:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The openssl extension in Ruby 2.x does not properly maintain the state of process memory after a file is reopened, which a

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruby-lang	Ruby	2.0	All	All	All

Application	Ruby-lang	Ruby	2.0.0	All	All	All
Application	Ruby-lang	Ruby	2.0.0	p0	All	All
Application	Ruby-lang	Ruby	2.0.0	p195	All	All
Application	Ruby-lang	Ruby	2.0.0	p247	All	All
Application	Ruby-lang	Ruby	2.0.0	preview1	All	All
Application	Ruby-lang	Ruby	2.0.0	preview2	All	All
Application	Ruby-lang	Ruby	2.0.0	rc1	All	All
Application	Ruby-lang	Ruby	2.0.0	rc2	All	All
Application	Ruby-lang	Ruby	2.1	-	All	All
Application	Ruby-lang	Ruby	2.1	preview1	All	All
Application	Ruby-lang	Ruby	2.1.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
castealer.rb · GitHub	af854a3a-2127-422b-91ae-364da26
Ruby OpenSSL private key spoofing? Hacker News	af854a3a-2127-422b-91ae-364da26
Full Disclosure: Ruby OpenSSL private key spoofing ~ CVE-2014-2734 with PoC	af854a3a-2127-422b-91ae-364da26
Dispute of Vulnerability CVE-2014-2734	af854a3a-2127-422b-91ae-364da26
castealer.rb analysis · GitHub	af854a3a-2127-422b-91ae-364da26
No Results Found ~ Packet Storm	af854a3a-2127-422b-91ae-364da26
GitHub - adrienthebo/cve-2014-2734: I think this CVE is full of lies and deceit and very confusing code.	af854a3a-2127-422b-91ae-364da26
Full Disclosure: Re: Ruby OpenSSL private key spoofing ~ CVE-2014-2734 with PoC	af854a3a-2127-422b-91ae-364da26
Malformed Request	af854a3a-2127-422b-91ae-364da26
www.osvdb.org/106006	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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