

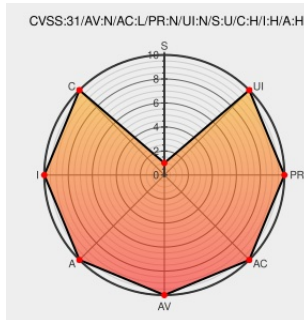


CVE-2011-4121

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:19 AM UTC

CVE-2011-4121

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ruby](#) from [Ruby-lang](#) contain the following vulnerability:

The OpenSSL extension of Ruby (Git trunk) versions after 2011-09-01 up to 2011-11-03 always generated an exponent value of '1' to be used for private RSA key generation. A remote attacker could use this flaw to bypass or corrupt integrity of services, depending on strong private RSA keys generation mechanism.

CVE-2011-4121 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **OpenSSL - OpenSSL extension of Ruby (Git trunk)** version = **versions after 2011-09-01 up to 2011-11-03**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

oss-security - CVE-2013-2228 : Salt Stack RSA exponent of 1 (there can be only one! da-na-naaah! na-na-na-naahh-nah-nahhh!)	Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2013/07/01/1
CVE-2011-4121	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2011-4121
CVE-2011-4121 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2011-4121
751800 – (CVE-2011-4121) CVE-2011-4121 ruby (openssl extension): Insecure way of creation exponent value by private RSA key generation	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-4121

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	Ruby-lang	Ruby	All	All	All	All
Application	Ruby-lang	Ruby	All	All	All	All
cpe:2.3:a:ruby-lang:ruby:*****:						
cpe:2.3:a:ruby-lang:ruby:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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