



CVE-2015-9097

Published on: 06/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9097

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

Certain versions of [Mail](#) from [Mail Project](#) contain the following vulnerability:

The mail gem before 2.5.5 for Ruby (aka A Really Ruby Mail Library) is vulnerable to SMTP command injection via CRLF sequences in a RCPT TO or MAIL FROM command, as demonstrated by CRLF sequences immediately before and after a DATA substring.

CVE-2015-9097 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Also unfold and split lazily - mikel/mail@72befdc · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/mikel/mail/commit/72befdc4dab3e6e288ce226a7da2aa474cf5be83

Third Party Advisory
www.mbsd.jp
application/pdf

MISC www.mbsd.jp/Whitepaper/smtpi.pdf

Rubysec

Issue Tracking
Vendor Advisory
web.archive.org
text/html
Inactive Link Not Archived

MISC rubysec.com/advisories/mail-OSVDB-131677

CVE-2015-9097: prevent SMTP command injection via To/From addresses by jeremy · Pull Request #1097 · mikel/mail · GitHub

Issue Tracking
Third Party Advisory
github.com
text/html

MISC github.com/mikel/mail/pull/1097

oss-security - CVE request: mail ruby gem <2.6.0 vulnerable to SMTP injection via recipient email addresses

Mailing List
Third Party Advisory
openwall.com
text/html

MISC openwall.com/lists/oss-security/2015/12/11/3

HackerOne

Issue Tracking
Third Party Advisory
hackerone.com
text/html

MISC hackerone.com/reports/137631

Add advisory for SMTP injection vulnerability in mail <2.6.0 · Issue #215 · rubysec/ruby-advisory-db · GitHub

Issue Tracking
Third Party Advisory
github.com
text/html

MISC github.com/rubysec/ruby-advisory-db/issues/215

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	Mail Project	Mail	All	All	All	All
cpe:2.3:a:mail_project:mail:*:*:*:*: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](#)