



# CVE-2015-0886

Published on: 02/27/2015 12:00:00 AM UTC

Last Modified on: 09/24/2021 01:15:00 PM UTC

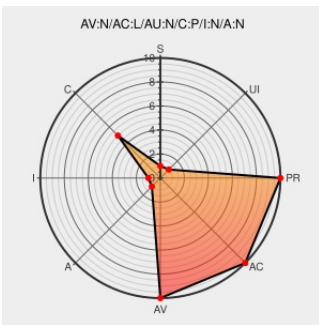
## CVE-2015-0886

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Fedora** from **Fedoraproject** contain the following vulnerability:

Integer overflow in the crypt\_raw method in the key-stretching implementation in jBCrypt before 0.4 makes it easier for remote attackers to determine cleartext values of password hashes via a brute-force attack against hashes associated with the maximum exponent.

CVE-2015-0886 has been assigned by vultures@jpcert.or.jp to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Pony Mail!	<a href="#">lists.apache.org</a> <a href="#">text/html</a>	MLIST [cassandra-commits] 20210924 [jira] [Created] (CASSANDRA-16990) Update jbcrypt library to 0.4 from 0.3m to resolve CVE-2015-0886
JVN#77718330: Vulnerability in the jBCrypt key stretching process	<a href="#">Third Party Advisory</a> <a href="#">Vendor Advisory</a> <a href="#">jvn.jp</a> <a href="#">text/xml</a>	JVN JVN#77718330
[SECURITY] Fedora 20 Update: jBCrypt-0.4-1.fc20	<a href="#">Third Party Advisory</a> <a href="#">lists.fedoraproject.org</a> <a href="#">text/html</a>	FEDORA FEDORA-2015-2994
2097 – if gensalt's log_rounds parameter is set to 31 it does 0 (ZERO) rounds!	<a href="#">Issue Tracking</a> <a href="#">Vendor Advisory</a> <a href="#">bugzilla.mindrot.org</a> <a href="#">text/html</a>	CONFIRM bugzilla.mindrot.org/show_bug.cgi?id=2097

mindrot.org projects weblog : /jBCrypt/news/rel04.html	<a href="#">text/html</a> <a href="#">Release Notes</a> <a href="#">Vendor Advisory</a> <a href="#">www.mindrot.org</a> <a href="#">text/xml</a>	 CONFIRM <a href="http://www.mindrot.org/projects/jBCrypt/news/rel04.html">www.mindrot.org/projects/jBCrypt/news/rel04.html</a>
Pony Mail!	<a href="#">lists.apache.org</a> <a href="#">text/html</a>	 MLIST [cassandra-commits] 20210924 [jira] [Commented] (CASSANDRA-16990) Update jbcrypt library to 0.4 from 0.3m to resolve CVE-2015-0886
Pony Mail!	<a href="#">lists.apache.org</a> <a href="#">text/html</a>	 MLIST [cassandra-commits] 20210924 [jira] [Updated] (CASSANDRA-16990) Update jbcrypt library to 0.4 from 0.3m to resolve CVE-2015-0886
[SECURITY] Fedora 22 Update: jBCrypt-0.4-1.fc22	<a href="#">Third Party Advisory</a> <a href="#">lists.fedoraproject.org</a> <a href="#">text/html</a>	 FEDORA FEDORA-2015-3120
[SECURITY] Fedora 21 Update: jBCrypt-0.4-1.fc21	<a href="#">Third Party Advisory</a> <a href="#">lists.fedoraproject.org</a> <a href="#">text/html</a>	 FEDORA FEDORA-2015-3032
<b>No Description Provided</b>	<a href="#">Third Party Advisory</a> <a href="#">VDB Entry</a> <a href="#">Vendor Advisory</a> <a href="#">jvndb.jvn.jp</a> <a href="#">text/html</a>	 JVNDB JVNDB-2015-000033

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](mailto: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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Application	<a href="#">Mindrot</a>	<a href="#">Jbcrypt</a>	All	All	All	All
Application	<a href="#">Mindrot</a>	<a href="#">Jbcrypt</a>	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:20:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:21:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:22:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:20:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:21:\*:\*:\*:\*:\*:

cpe:2.3:o:fedoraproject:fedora:22:\*:\*:\*:\*:\*:

cpe:2.3:a:mindrot:jbcrypt:\*:\*:\*:\*:\*:

cpe:2.3:a:mindrot:jbcrypt:\*:\*:\*:\*:\*:

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](#)**