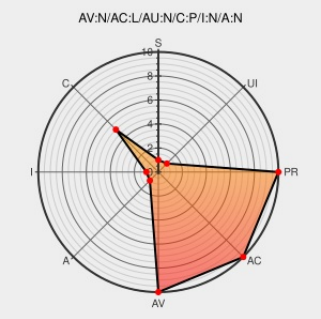
CVE-2015-0886

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
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	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	Third Party Advisory Vendor Advisory jvn.jp text/xml	JVN JVN#77718330
[SECURITY] Fedora 20 Update: jBCrypt-0.4-1.fc20	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2015-2994
2097 – if gensalt's log_rounds parameter is set to 31 it does 0 (ZERO) rounds!	Issue Tracking Vendor Advisory bugzilla.mindrot.org text/html	CONFIRM bugzilla.mindrot.org/show_bug.cgi?id=2097

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Mindrot	Jbcrypt	All	All	All	All
Application	Mindrot	Jbcrypt	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→