



# CVE-2020-28052

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-28052
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-18 01:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	An issue was discovered in Legion of the Bouncy Castle BC Java 1.65 and 1.66. The OpenSDBCrypt.checkPassword util

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition
Application	Apache	Karaf	4.3.2	All	All
Application	Apache	Solr	8.8.2	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.65	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.66	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.65	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	1.66	All	All
Application	Oracle	Banking Corporate Lending Process Management	14.2.0	All	All
Application	Oracle	Banking Corporate Lending Process Management	14.3.0	All	All
Application	Oracle	Banking Corporate Lending Process Management	14.5.0	All	All
Application	Oracle	Banking Credit Facilities Process Management	14.2.0	All	All
Application	Oracle	Banking Credit Facilities Process Management	14.3.0	All	All
Application	Oracle	Banking Credit Facilities Process Management	14.5.0	All	All
Application	Oracle	Banking Extensibility Workbench	14.2.0	All	All
Application	Oracle	Banking Extensibility Workbench	14.3.0	All	All
Application	Oracle	Banking Extensibility Workbench	14.5.0	All	All
Application	Oracle	Banking Supply Chain Finance	14.2.0	All	All
Application	Oracle	Banking Supply Chain Finance	14.3.0	All	All

Application	Oracle	Banking Supply Chain Finance	14.5.0	All	All
Application	Oracle	Banking Virtual Account Management	14.2.0	All	All
Application	Oracle	Banking Virtual Account Management	14.3.0	All	All
Application	Oracle	Banking Virtual Account Management	14.5.0	All	All
Application	Oracle	Blockchain Platform	All	All	All
Application	Oracle	Commerce Guided Search	11.3.2	All	All
Application	Oracle	Communications Application Session Controller	3.9m0p3	All	All
Application	Oracle	Communications Cloud Native Core Network Slice Selection Function	1.2.1	All	All
Application	Oracle	Communications Convergence	3.0.2.2.0	All	All
Operating System	Oracle	Communications Messaging Server	8.0.2	All	All
Operating System	Oracle	Communications Messaging Server	8.1	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.3.0	All	All
Application	Oracle	Communications Session Report Manager	All	All	All
Application	Oracle	Communications Session Route Manager	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All
Application	Oracle	Utilities Framework	4.3.0.6.0	All	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All	All
Application	Oracle	Utilities Framework	4.4.0.2.0	All	All
Application	Oracle	Utilities Framework	4.4.0.3.0	All	All
Application	Oracle	Webcenter Portal	11.1.1.9.0	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All
Application	Oracle	Webcenter Portal	12.2.1.4.0	All	All

## References

### Reference

[karaf-issues] 20210816 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.69 artifacts to mitigate CVE-2020-28052

Pony Mail!

CVE 2020 28052 · bcgit/bc-java Wiki · GitHub

Pony Mail!

Pony Mail!

[karaf-issues] 20210810 [jira] [Updated] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052

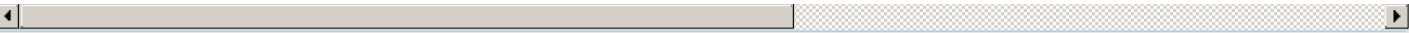
Pony Mail!

Pony Mail!
Oracle Critical Patch Update Advisory - April 2022
CyRC analysis: Authentication bypass vulnerability in Bouncy Castle
Pony Mail!
Pony Mail!
[karaf-issues] 20210816 [jira] [Updated] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
Pony Mail!
Oracle Critical Patch Update Advisory - July 2021
Pony Mail!
Pony Mail!
[karaf-issues] 20210810 [jira] [Commented] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
[karaf-issues] 20210817 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
bouncycastle.org
Oracle Critical Patch Update Advisory - October 2021
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - January 2022
[pulsar-commits] 20210406 [GitHub] [pulsar] lhotari commented on issue #9235: Upgrade Bounce Castle dependency on client to solve CVE-2
[solr-issues] 20210525 [jira] [Created] (SOLR-15431) Security vulnerability with Bouncy Castle library within Apache Solr 8.8.2
Pony Mail!
Pony Mail!
[karaf-issues] 20210810 [jira] [Created] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
Pony Mail!
[karaf-issues] 20210820 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
[karaf-issues] 20210817 [jira] [Commented] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
Pony Mail!
Pony Mail!
Pony Mail!
[karaf-issues] 20210824 [jira] [Commented] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
Pony Mail!
[karaf-issues] 20210824 [jira] [Resolved] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
Pony Mail!
Oracle Critical Patch Update Advisory - July 2022
Oracle Critical Patch Update Advisory - April 2021
Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[150588](#) Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2022)

[375482](#) Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2021)

[690058](#) Free Berkeley Software Distribution (FreeBSD) Security Update for bouncycastle15 (70e71a24-0151-11ec-bf0c-080027eedc6a)

[87524](#) Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2022)

[980329](#) Java (maven) Security Update for org.bouncycastle:bcprov-ext-jdk16 (GHSA-73xv-w5gp-frxh)

© [CVE.report](#) 2026 |

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](#)