



CVE-2018-1000613

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1000613
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-09 20:29:00 UTC
Updated	2024-01-25 02:15:00 UTC
Description	Legion of the Bouncy Castle Legion of the Bouncy Castle Java Cryptography APIs 1.58 up to but not including 1.60 contain

Risk And Classification

Problem Types: CWE-470

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-cryptography-api	All	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	Banking Platform	2.6.0	All	All	All
Application	Oracle	Banking Platform	2.6.1	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Business Process Management Suite	11.1.1.9.0	All	All	All
Application	Oracle	Business Process Management Suite	12.1.3.0.0	All	All	All
Application	Oracle	Business Process Management Suite	12.2.1.3.0	All	All	All
Application	Oracle	Business Transaction Management	12.1.0	All	All	All
Application	Oracle	Communications Application Session Controller	3.7.1	All	All	All
Application	Oracle	Communications Application Session Controller	3.8.0	All	All	All
Application	Oracle	Communications Converged Application Server	All	All	All	All
Application	Oracle	Communications Converged Application Server	7.0.0.1	All	All	All
Application	Oracle	Communications Convergence	3.0.2	All	All	All

Application	Oracle	Communications Diameter Signaling Router	8.0.0	All	All	All
Application	Oracle	Communications Diameter Signaling Router	8.1	All	All	All
Application	Oracle	Communications Diameter Signaling Router	8.2	All	All	All
Application	Oracle	Communications Diameter Signaling Router	8.2.1	All	All	All
Application	Oracle	Communications Webrtc Session Controller	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	7.2	All	All	All
Application	Oracle	Data Integrator	12.2.1.3.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	12.1.0.5.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.2.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.3.0.0	All	All	All
Application	Oracle	Enterprise Manager For Fusion Middleware	13.2.0.0	All	All	All
Application	Oracle	Enterprise Manager For Fusion Middleware	13.3.0.0	All	All	All
Application	Oracle	Enterprise Repository	11.1.1.7.0	All	All	All
Application	Oracle	Enterprise Repository	12.1.3.0.0	All	All	All
Application	Oracle	Managed File Transfer	12.1.3.0.0	All	All	All
Application	Oracle	Managed File Transfer	12.2.1.3.0	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Retail Convenience And Fuel Pos Software	2.8.1	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Soa Suite	12.1.3.0.0	All	All	All
Application	Oracle	Soa Suite	12.2.1.3.0	All	All	All
Application	Oracle	Utilities Network Management System	1.12.0.3	All	All	All
Application	Oracle	Utilities Network Management System	2.3.0.0	All	All	All
Application	Oracle	Utilities Network Management System	2.3.0.1	All	All	All
Application	Oracle	Utilities Network Management System	2.3.0.2	All	All	All
Application	Oracle	Webcenter Portal	11.1.1.9.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache.org

added full filtering for BDS data. · bcgit/bc-java@cd98322 · GitHub	CONFIRM	github.com
[security-announce] openSUSE-SU-2020:0607-1: moderate: Security update f	SUSE	lists.opensuse.org
added additional checking to XMSS BDS tree parsing. Failures now most... · bcgit/bc-java@4092ede · GitHub	CONFIRM	github.com
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com
September 2018 Bouncy Castle Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com
Pony Mail!		lists.apache.org
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[690581](#) Free Berkeley Software Distribution (FreeBSD) Security Update for several security defects in the bouncy castle crypto apis (fe93803c-883f-11e8-9f0c-001b216d295b)

[982266](#) Java (maven) Security Update for org.bouncycastle:bcprov-jdk15 (GHSA-4446-656p-f54g)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report