CVE-2018-1000180

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-1000180
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-05 13:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	Bouncy Castle BC 1.54 - 1.59, BC-FJA 1.0.0, BC-FJA 1.0.1 and earlier have a flaw in the Low-level interface to RSA key pa

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bouncycastle	Fips Java Api	All	All	All	All
Application	Bouncycastle	Legion-of-the-bouncy-castle-java-crytography-api	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	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 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	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 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	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	All	All	All	All
Application	Oracle	Enterprise Repository	12.1.3.0.0	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	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	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 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	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	Soa Suite	12.1.3.0.0	All	All	All
Application	Oracle	Soa Suite	12.2.1.3.0	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	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	12.1.3.0.0	All	All	All
Application	Oracle	Weblogic Server	12.1.3.0.0	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1.0	All	All	All
Operating System	Redhat	Virtualization	4.2	All	All	All
Operating System	Redhat	Virtualization	4.2	All	All	All

References

Reference	Source	Link	Tags
BJA-694 cleaned up primality test · bcgit/bc-java@73780ac · GitHub	CONFIRM	github.com	Patch
CVE 2018 1000180 · bcgit/bc-java Wiki · GitHub	MISC	github.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Pony Mail!		lists.apache.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
Debian -- Security Information -- DSA-4233-1 bouncycastle	DEBIAN	www.debian.org	Third
Bountysource	MISC	www.bountysource.com	Third
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
BJA-694 minor tweak to avoid method signature change · bcgit/bc-java@22467b6 · GitHub	CONFIRM	github.com	Patch
September 2018 Bouncy Castle Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Patch
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com	Patch
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Pony Mail!	MLIST	lists.apache.org	
Bouncy Castle CVE-2018-1000180 Security Weakness	BID	www.securityfocus.com	Third
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

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)

982263 Java (maven) Security Update for org.bouncycastle:bcprov-jdk15 (GHSA-xqj7-j8j5-f2xr)

© 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 registred 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.

Free CVE JSON API cve.report/api

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