



CVE-2019-3740

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

Summary

CVE	CVE-2019-3740
State	PUBLIC
Assigner	secure@dell.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-18 23:15:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Information Exposure Through Timing Discrepancy vulner

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Bsafe Cert-j	All	All	All	All
Application	Dell	Bsafe Crypto-j	All	All	All	All
Application	Dell	Bsafe Ssl-j	All	All	All	All
Application	Oracle	Application Performance Management	13.3.0.0	All	All	All
Application	Oracle	Application Performance Management	13.4.0.0	All	All	All
Application	Oracle	Communications Network Integrity	7.3.2	All	All	All
Application	Oracle	Communications Network Integrity	7.3.5	All	All	All
Application	Oracle	Communications Network Integrity	7.3.6	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.3.2	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.3.4	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.3.5	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.0	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.1	All	All	All
Application	Oracle	Database	12.1.0.2	All	All	All
Application	Oracle	Database	12.2.0.1	All	All	All
Application	Oracle	Database	18c	All	All	All
Application	Oracle	Database	19c	All	All	All

Application	Oracle	Global Lifecycle Management Opatch	All	All	All	All
Application	Oracle	Goldengate	All	All	All	All
Application	Oracle	Retail Assortment Planning	15.0.3.0	All	All	All
Application	Oracle	Retail Assortment Planning	16.0.3.0	All	All	All
Application	Oracle	Retail Integration Bus	14.1	All	All	All
Application	Oracle	Retail Integration Bus	15.0	All	All	All
Application	Oracle	Retail Integration Bus	16.0	All	All	All
Application	Oracle	Retail Predictive Application Server	14.1.3.0	All	All	All
Application	Oracle	Retail Predictive Application Server	15.0	All	All	All
Application	Oracle	Retail Predictive Application Server	15.0.3.0	All	All	All
Application	Oracle	Retail Predictive Application Server	16.0.3.0	All	All	All
Application	Oracle	Retail Service Backbone	14.1	All	All	All
Application	Oracle	Retail Service Backbone	15.0	All	All	All
Application	Oracle	Retail Service Backbone	16.0	All	All	All
Application	Oracle	Retail Store Inventory Management	14.0.4	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1.3	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0.3	All	All	All
Application	Oracle	Retail Store Inventory Management	16.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	15.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0.5	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	18.0.2	All	All	All
Application	Oracle	Retail Xstore Point Of Service	19.0.1	All	All	All
Application	Oracle	Storagetek Acsls	8.5.1	All	All	All
Application	Oracle	Storagetek Tape Analytics Sw Tool	2.3	All	All	All
Application	Oracle	Weblogic Server	10.3.6.0.0	All	All	All
Application	Oracle	Weblogic Server	12.1.3.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
Application	Rsa	Bsafe Cert-j	All	All	All	All
Application	Rsa	Bsafe Crypto-j	All	All	All	All
Application	Rsa	Bsafe Crypto-j	All	All	All	All
Application	Rsa	Bsafe Ssl-j	All	All	All	All

References

Reference	Source	Link	Tags
Access Denied	MISC	www.dell.com	Third Party Advisory
Oracle Critical Patch Update Advisory - July 2020	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com	
Access Denied		www.dell.com	
Access Denied	MITRE	www.dell.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

20215 Oracle Database 19c Critical Patch Update - April 2021
20216 Oracle Database 18c Critical Patch Update - April 2021
20217 Oracle Database 12.2.0.1 Critical Patch Update - April 2021
20218 Oracle Database 12.2.0.1 Critical Patch Update - April 2021 (Unauthenticated)
20219 Oracle Database 12.1.0.2 Critical Patch Update - April 2021
20220 Oracle Database 12.1.0.2 Critical Patch Update - April 2021 (Unauthenticated)
20275 Oracle Database 18c Critical OJVM Patch Update - April 2021
20278 Oracle Database 19c Critical OJVM Patch Update - April 2021
20304 Oracle Database 12.2.0.1 Critical OJVM Patch Update - April 2021
375484 Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2021) (WebLogic Server Unix Authentication Record)
730241 Oracle GoldenGate October 2021 Critical Patch Update (GPUOCT2021)
87448 Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2021)

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](#)