



CVE-2016-8217

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

Summary

CVE	CVE-2016-8217
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-03 07:59:00 UTC
Updated	2021-12-16 18:44:00 UTC
Description	EMC RSA BSAFE Crypto-J versions prior to 6.2.2 has a PKCS#12 Timing Attack Vulnerability. A possible timing attack cou

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Bsafe Crypto-j	All	All	All	All
Application	Dell	Bsafe Crypto-j	All	All	All	All
Application	Emc	Rsa Bsafe Crypto-j	All	All	All	All

References

Reference
SecurityFocus
EMC RSA BSAFE Crypto-J Security Bypass and Information Disclosure Vulnerabilities
RSA BSAFE Crypto-J Bugs Let Remote USers Bypass OCSP Time Validation and Conduct Timing Attacks to Determine PKCS MAC Values
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)