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.