CVE-2013-6078

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

Summary

CVE	CVE-2013-6078
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-17 15:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The default configuration of EMC RSA BSAFE Toolkits and RSA Data Protection Manager (DPM) 20130918 uses the Dual

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:N

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Rsa Bsafe Toolkits	-	All	All	All

Application	Emc	Rsa Data Protection Manager	20130918	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Stop using NSA-influenced code in our products, RSA tells customers | Ars Technica	af854a3a-2127-422b-91ae-364da2661108
In Wake of Latest Crypto Revelations, 'Everything is Suspect' | Threatpost	af854a3a-2127-422b-91ae-364da2661108
RSA: Don’t Use Encryption Influenced by NSA - Wall Street Journal - WSJ.com	af854a3a-2127-422b-91ae-364da2661108
A Few Thoughts on Cryptographic Engineering: RSA warns developers not to use RSA products	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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