CVE-2007-6755

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-6755
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-11 22:55:00 UTC
Updated	2022-11-01 14:44:00 UTC
Description	The NIST SP 800-90A default statement of the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG)

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Bsafe Crypto-c-micro-edition	All	All	All	All
Application	Dell	Bsafe Crypto-j	5.0	All	All	All
Application	Dell	Bsafe Crypto-j	5.0.1	All	All	All
Application	Dell	Bsafe Crypto-j	All	All	All	All
Application	Dell	Bsafe Crypto-j Jsafe And Jce	5.0	All	All	All
Application	Dell	Bsafe Crypto-j Jsafe And Jce	5.0.1	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.1	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.14	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.15	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.16	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.19	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.1	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.14	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.15	All	All	All
Application	Rsa	Bsafe Crypto-c Me	3.0.0.16	All	All	All

Application	Rsa	Bsafe Crypto-c Me	3.0.0.19	All	All	All
Application	Rsa	Bsafe Crypto-c Me	All	All	All	All
Application	Rsa	Bsafe Crypto-c Me Mfp Psos	3.0.0.1	All	All	All
Application	Rsa	Bsafe Crypto-c Me Mfp Psos	3.0.0.1	All	All	All
Application	Rsa	Bsafe Crypto-c Me Mfp Psos	All	All	All	All
Application	Rsa	Bsafe Crypto-c Me Mfp Vxworks	All	All	All	All
Application	Rsa	Bsafe Crypto-j	All	All	All	All
Application	Rsa	Bsafe Crypto-j Jsafe And Jce	5.0	All	All	All
Application	Rsa	Bsafe Crypto-j Jsafe And Jce	5.0.1	All	All	All
Application	Rsa	Bsafe Crypto-j Jsafe And Jce	5.0	All	All	All
Application	Rsa	Bsafe Crypto-j Jsafe And Jce	5.0.1	All	All	All
Application	Rsa	Bsafe Crypto-j Jsafe And Jce	All	All	All	All

References

Reference	Source	Link
In Wake of Latest Crypto Revelations, 'Everything is Suspect' | Threatpost	MISC	threatpost.com
Stop using NSA-influenced code in our products, RSA tells customers | Ars Technica	MISC	arstechnica.com
Dual Elliptic Curve Deterministic Random Bit Generation Predictable Random Number Generator Weakness	BID	www.securityfocu
A Few Thoughts on Cryptographic Engineering: RSA warns developers not to use RSA products	MISC	blog.cryptography
Schneier on Security: The Strange Story of Dual_EC_DRBG	MISC	www.schneier.cor
rump2007.cr.yp.to/15-shumow.pdf	MISC	rump2007.cr.yp.to
RSA: Don't Use Encryption Influenced by NSA - Wall Street Journal - WSJ.com	MISC	stream.wsj.com
A Few Thoughts on Cryptographic Engineering: The Many Flaws of Dual_EC_DRBG	MISC	blog.cryptography
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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