CVE-2014-4630

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-4630
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-30 15:59:00 UTC
Updated	2021-12-09 18:31:00 UTC
Description	EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x before 4.0.6 and RSA BSAFE SSL-J before 6.1.4 do not ensure that a s

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Bsafe	4.0.0	All	All	All
Application	Dell	Bsafe	4.0.1	All	All	All
Application	Dell	Bsafe	4.0.2	All	All	All
Application	Dell	Bsafe	4.0.3	All	All	All
Application	Dell	Bsafe	4.0.4	All	All	All
Application	Dell	Bsafe	4.0.5	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.0	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.1	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.2	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.3	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.4	All	All	All
Application	Dell	Bsafe Micro-edition-suite	4.0.5	All	All	All
Application	Dell	Bsafe Ssl-j	All	All	All	All
Application	Emc	Rsa Bsafe	4.0.0	All	All	All
Application	Emc	Rsa Bsafe	4.0.1	All	All	All
Application	Emc	Rsa Bsafe	4.0.2	All	All	All
Application	Emc	Rsa Bsafe	4.0.3	All	All	All

Application	Emc	Rsa Bsafe	4.0.4	All	All	All
Application	Emc	Rsa Bsafe	4.0.5	All	All	All
Application	Emc	Rsa Bsafe	4.0.0	All	All	All
Application	Emc	Rsa Bsafe	4.0.1	All	All	All
Application	Emc	Rsa Bsafe	4.0.2	All	All	All
Application	Emc	Rsa Bsafe	4.0.3	All	All	All
Application	Emc	Rsa Bsafe	4.0.4	All	All	All
Application	Emc	Rsa Bsafe	4.0.5	All	All	All
Application	Emc	Rsa Bsafe Ssl-j	All	All	All	All

References

Reference	Source	Link
Triple Handshakes Considered Harmful: Breaking and Fixing Authentication over TLS	MISC	secure-resumption.com
20141230 ESA-2014-158: RSA BSAFE Micro Edition Suite and SSL-J Triple Handshake Vulnerability	BUGTRAQ	archives.neohapsis.com
Multiple EMC Products CVE-2014-4630 Man in the Middle Security Bypass Vulnerability	BID	www.securityfocus.com
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.