



CVE-2016-0923

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

Summary

CVE	CVE-2016-0923
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-18 02:59:00 UTC
Updated	2021-12-16 18:44:00 UTC
Description	The client in EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x before 4.0.9 and 4.1.x before 4.1.5 places the weakest algo

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dell	Bsafe	All	All	All	All
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	4.0.7	All	All	All
Application	Dell	Bsafe	4.0.8	All	All	All
Application	Dell	Bsafe	4.1.0	All	All	All
Application	Dell	Bsafe	4.1.1	All	All	All
Application	Dell	Bsafe	4.1.2	All	All	All
Application	Dell	Bsafe	4.1.3	All	All	All
Application	Dell	Bsafe	4.1.4	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	4.0.6	All	All	All
Application	Emc	Rsa Bsafe	4.0.7	All	All	All
Application	Emc	Rsa Bsafe	4.0.8	All	All	All
Application	Emc	Rsa Bsafe	4.1.0	All	All	All
Application	Emc	Rsa Bsafe	4.1.1	All	All	All
Application	Emc	Rsa Bsafe	4.1.2	All	All	All
Application	Emc	Rsa Bsafe	4.1.3	All	All	All
Application	Emc	Rsa Bsafe	4.1.4	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	4.0.6	All	All	All
Application	Emc	Rsa Bsafe	4.0.7	All	All	All
Application	Emc	Rsa Bsafe	4.0.8	All	All	All
Application	Emc	Rsa Bsafe	4.1.0	All	All	All
Application	Emc	Rsa Bsafe	4.1.1	All	All	All
Application	Emc	Rsa Bsafe	4.1.2	All	All	All
Application	Emc	Rsa Bsafe	4.1.3	All	All	All
Application	Emc	Rsa Bsafe	4.1.4	All	All	All

References

Reference

EMC RSA BSAFE Micro Edition Suite Security Weakness and Information Disclosure Vulnerabilities

Bugtraq: ESA-2016-094: RSA BSAFE® Micro Edition Suite Multiple Vulnerabilities

RSA BSAFE Micro Edition Suite Weak Signature Support Allows Weak Signature Algorithm Negotiation and Exposes Users to Hash Collision

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)