



CVE-2016-3019

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

Summary

CVE	CVE-2016-3019
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-07 17:29:00 UTC
Updated	2020-10-27 11:37:00 UTC
Description	IBM Security Access Manager for Web 9.0.0 uses weaker than expected cryptographic algorithms that could allow an attac

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Ibm	Security Access Manager 9.0 Firmware	All	All	All	All
Operating System	Ibm	Security Access Manager 9.0 Firmware	All	All	All	All

References

Reference

IBM Security Access Manager Appliance Weak Password Encryption Algorithm Lets Remote Authenticated Users Obtain Potentially Sensitive
IBM Security Access Manager Products CVE-2016-3019 Information Disclosure Vulnerability
Security Bulletin: IBM Security Access Manager appliances use some weak cryptographic algorithms for stash file encryption (CVE-2016-3019)
IBM X-Force Exchange
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](#)