CVE-2015-5013

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

Summary

CVE	CVE-2015-5013
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-08 19:59:00 UTC
Updated	2021-11-09 20:08:00 UTC
Description	The IBM Security Access Manager appliance includes configuration files that contain obfuscated plaintext-passwords which

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ibm	Security Access Manager 9.0	-	All	All	All
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
Application	Ibm	Security Access Manager For Mobile	All	All	All	All
Application	Ibm	Security Access Manager For Mobile	All	All	All	All
Hardware	Ibm	Security Access Manager For Mobile Appliance	8.0	All	All	All
Hardware	Ibm	Security Access Manager For Mobile Appliance	8.0	All	All	All
Operating System	Ibm	Security Access Manager For Web 8.0 Firmware	All	All	All	All
Operating System	Ibm	Security Access Manager For Web 8.0 Firmware	All	All	All	All
Hardware	Ibm	Security Access Manager For Web Appliance	8.0	All	All	All
Hardware	Ibm	Security Access Manager For Web Appliance	8.0	All	All	All

References

Reference
IBM Security Access Manager Lets Local Users View Passwords Stored in Configuration Files - SecurityTracker
IBM Security Access Manager Products CVE-2015-5013 Information Disclosure Vulnerability
IBM Security Bulletin: IBM Security Access Manager uses configuration files with obfuscated passwords that can be accessed by authenticate

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.

Free CVE JSON API cve.report/api

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