



CVE-2016-3029

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-3029 |
| State | PUBLIC |
| Assigner | psirt@us.ibm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-02-01 20:59:00 UTC |
| Updated | 2020-10-27 11:37:00 UTC |
| Description | IBM Security Access Manager for Web is vulnerable to cross-site request forgery which could allow an attacker to execute i |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---|---------|--------|---------|----------|
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.0 | All | All | All |
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.0 | All | All | All |
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager 9.0 Firmware | 9.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.5 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.4 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.3 | All | All | All |

| | | | | | | |
|------------------|-----|---|---------|-----|-----|-----|
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.0.5 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Mobile 8.0 Firmware | 8.0.1.4 | 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 | 8.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.5 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.4 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.1 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.0.5 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.0 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.2 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.3 | All | All | All |
| Operating System | ibm | Security Access Manager For Web 8.0 Firmware | 8.0.1.4 | 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 Products CVE-2016-3029 Cross Site Request Forgery Vulnerability](#)

[IBM Security Bulletin: IBM Security Access Manager appliances are affected by a cross-site request forgery \(CSRF\) vulnerability \(CVE-2016-3029\)](#)

[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](#).

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