



CVE-2018-15780

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

Summary

CVE	CVE-2018-15780
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-03 21:29:00 UTC
Updated	2019-10-09 23:35:00 UTC
Description	RSA Archer versions prior to 6.5.0.1 contain an improper access control vulnerability. A remote malicious user could potent

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsa	Archer Grc Platform	All	All	All	All
Application	Rsa	Archer Grc Platform	All	All	All	All

References

Reference	Source	Link	Ta
Full Disclosure: DSA-2018-224:RSA Archer GRC Platform Improper Access Control Vulnerability	FULLDISC	seclists.org	Me
EMC RSA Archer GRC Platform CVE-2018-15780 Access Bypass Vulnerability	BID	www.securityfocus.com	Th
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

LEGACY: RSA would like to thank Sam Sayen for reporting this vulnerability.

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](#)