



CVE-2018-19505

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

Summary

CVE	CVE-2018-19505
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-03 19:29:00 UTC
Updated	2019-02-15 15:03:00 UTC
Description	Remedy AR System Server in BMC Remedy 7.1 may fail to set the correct user context in certain impersonation scenarios,

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bmc	Remedy Action Request System Server	7.1	All	All	All
Application	Bmc	Remedy Action Request System Server	7.1	All	All	All

References

Reference

BMC Remedy 7.1 User Impersonation ≈ Packet Storm

BMC Remedy Action Request System Flaw Lets Remote Authenticated Users Modify Certain User Data on the Target System - SecurityTrack

Full Disclosure: CVE-2018-19505 - Impersonation may lead to incorrect user context in Remedy AR System Server in BMC Remedy 7.1

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.

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