



CVE-2018-6959

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

Summary

CVE	CVE-2018-6959
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-13 13:29:00 UTC
Updated	2018-05-17 17:43:00 UTC
Description	VMware vRealize Automation (vRA) prior to 7.4.0 contains a vulnerability in the handling of session IDs. Exploitation of this

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vrealize Automation	All	All	All	All
Application	Vmware	Vrealize Automation	All	All	All	All

References

Reference	Source
VMSA-2018-0009	CONFIR
VMware vRealize Automation Bugs Let Remote Users Hijack Sessions and Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTR
Malformed Request	BID
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

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