

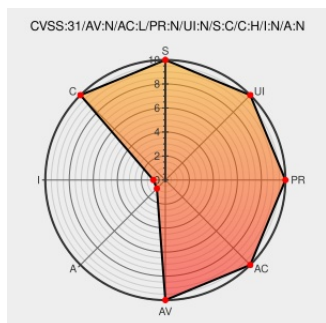


CVE-2020-3944

Published on: 02/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3944

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) has an improper trust store configuration leading to authentication bypass. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may be able to bypass Adapter authentication.

CVE-2020-3944 has been assigned by [vmw](#) security@vmware.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [vmw](#) **VMWare - vRealize Operations for Horizon Adapter** version **6.7.x prior to 6.7.1**

Affected Vendor/Software: [vmw](#) **VMWare - vRealize Operations for Horizon Adapter** version **6.6.x prior to 6.6.1**

CVSS3 Score: **8.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Taas	Link
-------------	------	------

CONFIRM www.vmware.com/security/advisories/VMSA-2020-0003.html

text/html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Vmware	Vrealize Operations	All	All	All	All
Application	Vmware	Vrealize Operations	All	All	All	All
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:a:vmware:vrealize_operations:*:*:*:*:horizon:*:*						
cpe:2.3:a:vmware:vrealize_operations:*:*:*:*:horizon:*:*						

Next ID→

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