



CVE-2018-6979

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-6979
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-05 12:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	The VMware Workspace ONE Unified Endpoint Management Console (A/W Console) 9.7.x prior to 9.7.0.3, 9.6.x prior to 9.6.0.3

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Airwatch Console	All	All	All	All
Application	Vmware	Airwatch Console	All	All	All	All

References

Reference

- VMware Workspace ONE Unified Endpoint Management Console Lets Remote Users Bypass SAML Authentication on the Target System - Security Bulletin SMLB-2018-0024
- VMSA-2018-0024.1
- 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.

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](#)