National Security Agency | Cybersecurity Advisory

Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials

Summary

Russian state-sponsored malicious cyber actors are exploiting a vulnerability in VMware®[1] Access and VMware Identity Manager[2] products [1], allowing the actors access to protected data and abusing federated authentication. VMware released a patch for the Command Injection Vulnerability captured in CVE-2020-4006 on December 3rd 2020. NSA encourages National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) network administrators to prioritize mitigation of the vulnerability on affected servers.

Password-based access to the web-based management interface of the device is required to exploit the vulnerability, so using a strong and unique password lowers the risk of exploitation. The risk is lowered further if the web-based management interface is not accessible from Internet. The vulnerability affects the following products [2]:

- VMware Access®[3] 20.01 and 20.10 on Linux®[4]
- VMware vIDM®[5] 3.3.1, 3.3.2, and 3.3.3 on Linux
- VMware vIDM Connector 3.3.1, 3.3.2, 3.3.3, 19.03
- VMware Cloud Foundation®[6] 4.x
- VMware vRealize Suite Lifecycle Manager®[7] 8.x

The exploitation (T1190[8]) via command injection (T1059) led to installation of a web shell (T1505.003) and follow-on malicious activity where credentials in the form of SAML authentication assertions were generated and sent to Microsoft®[9] Active Directory Federation Services (ADFS) (T1212), which in turn granted the actors access to protected data (TA0009).

It is critical when running products that perform authentication that the server and all the services that depend on it are properly configured for secure operation and integration. Otherwise, SAML assertions could be forged, granting access to numerous resources. If integrating authentication servers with ADFS, NSA recommends following Microsoft's best practices, especially for securing SAML assertions and requiring multi-factor authentication [3] [4].

Mitigation Actions

Patch

Update affected systems to the latest version as soon as possible according to VMware's instructions at KB81754 [1] [5]. Review and harden configurations and monitoring of federated authentication providers.

[1] VMware® is a registered trademark of VMware, Inc.
[2] VMware® Workspace ONE Access, formerly VMware Identity Manager (vIDM), are noted throughout as VMware Access or vIDM
[3] VMware Access® is a registered trademark of VMware, Inc.
[4] Linux® is a registered trademark of Linus Torvalds.
[5] VMware vIDM® is a registered trademark of VMware, Inc.
[6] VMware Cloud Foundation® is a registered trademark of VMware, Inc.
[7] VMware vRealize Suite Lifecycle Manager® is a registered trademark of VMware, Inc.
[8] T1190 and similar references are MITRE® ATT&CK® techniques and tactics. MITRE and ATT&CK are registered trademarks of The MITRE Corporation.
[9] Microsoft® is a registered trademark of Microsoft Corporation.

Workaround

According to VMware's Knowledge Base article KB81731, critical portions of this activity can be blocked by disabling the configurator service using the following procedures for Linux-based appliances [6]:

1. Use ssh to connect to the appliance using "`sshuser`" credentials configured during installation or when updated later.

2. Switch to root by typing `su` and provide "`root`" credentials configured during installation or when updated later.

3. Run the following commands:

```
cd /opt/vmware/horizon/workspace
mkdir webapps.tmp
mv conf/Catalina/localhost/cfg.xml webapps.tmp
service horizon-workspace restart
```

4. Repeat steps for all Linux-based appliances affected by CVE-2020-4006.

For Windows-based servers:

1. Log in as Administrator.

2. Open a Command Prompt window and run the following commands:

```
net stop "VMwareIDMConnector"
cd \VMware\VMwareIdentityManager\Connector\opt\vmware\horizon\workspace
mkdir webappstmp
move webapps\cfg webappstmp
move conf\Catalina\localhost\cfg.xml webappstmp
net start "VMwareIDMConnector"
```

3. Repeat steps for all Windows-based servers affected by CVE-2020-4006.

VMware's KB81731 lists steps to revert the workaround if needed.

This workaround should only be a temporary fix until able to fully patch the system. In addition, review and harden configurations and monitoring of federated authentication providers.

Detection

Network-based indicators are unlikely to be effective at detecting exploitation since the activity occurs exclusively inside an encrypted transport layer security (TLS) tunnel associated with the web interface. However, indications of this activity may be caught in server logs. The presence of an "exit" statement followed by any 3-digit number, such as "exit 123", within the configurator.log would suggest that exploitation activity may have occurred on the system. This log can be found at /opt/vmware/horizon/workspace/logs/configurator.log on the server. Other commands along with encoded scripts may also be present. If such logs are detected, incident response actions should be followed. Additional investigation of the server, especially for web shell malware, is recommended (see the NSA CSI "Detect and Prevent Web Shell Malware" [7]).

Regularly monitor authentication logs for anomalous authentications, especially successful ones that leverage established trusts but that come from unusual addresses or contain unusual properties.

Further Guidance

Exploiting the vulnerability requires authenticated password-based access to the management interface of the device, which is encrypted with TLS. That interface typically runs over port 8443, but it could be over any user-defined port. NSA recommends that NSS, DoD, and DIB network administrators limit the accessibility of the management interface on servers to only a small set of known systems and block it from direct Internet access (see “Performing Out-of-Band Management” [8]).

Since the server requires that passwords be intentionally chosen upon installation, there are no known default passwords. Setting the password to a strong unique password would make it more difficult to exploit, but would likely not mitigate an existing compromise.

It is critical when running products that perform authentication that the server and all the services that depend on it are properly configured for secure operation and integration. Otherwise, SAML assertions could be forged, granting access to numerous resources. If integrating authentication servers with ADFS, NSA recommends following Microsoft’s best practices, especially for securing SAML assertions and requiring multi-factor authentication [3] [4].

Works Cited

[1] VMware patch KB81754. [Online] Available at: https://kb.vmware.com/s/article/81754
[2] VMware. VMware Security Advisory VMSA-2020-0027. [Online] Available at: https://www.vmware.com/security/advisories/VMSA-2020-0027.html
[3] Microsoft. Best practices for securing Active Directory Federation Services. [Online] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs
[4] Microsoft. Best Practices for Secure Planning and Deployment of AD FS. [Online] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/best-practices-for-secure-planning-and-deployment-of-ad-fs
[5] NSA. Update and Upgrade Software Immediately. [Online] Available at: https://www.nsa.gov/cybersecurity-guidance
[6] VMware. WMware Workspace ONE Access, VMware Identity Manager, VMware Identity Manager Connector Workaround Instructions for CVE-2020-4006 (81731). [Online] Available at: https://kb.vmware.com/s/article/81731
[7] NSA. Detect and Prevent Web Shell Malware. [Online] Available at: https://www.nsa.gov/cybersecurity-guidance
[8] NSA. Performing Out-of-Band Network Management. [Online] Available at: https://www.nsa.gov/cybersecurity-guidance

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA’s cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov