Hive Pro

Threat Level

Amber

THREAT ADVISORY

# VULNERABILITY REPORT

## VMware products impacted by an authentication bypass vulnerability and other flaws

| Date of Publication | Admiralty code | TA Number |
| --- | --- | --- |
| August 4, 2022 | A1 | TA2022163 |

# Summary

VMware has addressed multiple vulnerabilities, including an authentication bypass (CVE-2022-31656), remote code execution (CVE-2022-31658, CVE-2022-31659, and CVE-2022-31665), and many more flaws.

## CVE Table

| CVE | NAME | PATCH |
|---|---|---|
| CVE-2022-31656 | Authentication Bypass Vulnerability | ✓ |
| CVE-2022-31658 | JDBC Injection Remote Code Execution Vulnerability | ✓ |
| CVE-2022-31659 | SQL injection Remote Code Execution Vulnerability | ✓ |
| CVE-2022-31660 | Local Privilege Escalation Vulnerability | ✓ |
| CVE-2022-31661 | Local Privilege Escalation Vulnerability | ✓ |
| CVE-2022-31664 | Local Privilege Escalation Vulnerability | ✓ |
| CVE-2022-31665 | JDBC Injection Remote Code Execution Vulnerability | ✓ |
| CVE-2022-31657 | URL Injection Vulnerability | ✓ |
| CVE-2022-31662 | Path traversal vulnerability | ✓ |
| CVE-2022-31663 | Cross-site scripting (XSS) vulnerability | ✓ |

# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0040**<br>Impact | **TA0005**<br>Defense Evasion | **T1556**<br>Modify Authentication Process | **TA0004**<br>Privilege Escalation |
| **T1055**<br>Process Injection | **T1068**<br>Exploitation for Privilege Escalation | **TA0003**<br>Persistence | **TA0002**<br>Execution |
| **T1059**<br>Command and Scripting Interpreter | **TA0001**<br>Initial Access | **T1190**<br>Exploit Public-Facing Application | |

# Technical Details

**#1**

CVE-2022-31656, an authentication bypass vulnerability that affects the local domain users, is the most critical flaw(as per VMware). A remote attacker with access to the user interface can acquire administrative rights without a need to authenticate.

**#2**

The remote code execution vulnerabilities (CVE-2022-31658 and CVE-2022-31665) are caused due to improper input validation while dealing with JDBC strings. An SQL injection(CVE-2022-31659) flaw could lead to remote code execution due to insufficient sanitization of user-supplied data.

**#3**

A URL injection vulnerability (CVE-2022-31657) may allow a remote attacker to conduct a phishing attack and steal potentially sensitive information. A path traversal vulnerability (CVE-2022-31662) could allow the remote attacker to read arbitrary files on the system. A Cross-site scripting vulnerability (CVE-2022-31663) would allow an attacker with some user interaction to insert JavaScript code in the target user's window due to incorrect user input sanitization.

**#4**

Finally, local privilege escalation vulnerabilities (CVE-2022-31660, CVE-2022-31661, and CVE-2022-31664) exist due to incorrect privilege management, allowing an actor with local access to raise privileges to root.

# Vulnerability Details

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2022-31656 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1, VMware Identity Manager: 3.3.4 - 3.3.6, vRealize Automation: 7.6, vRealize Suite Lifecycle Manager: 8.0 - 8.4.1 and Cloud Foundation: 4.2 - 4.4 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:identity_manager:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:vrealize_automation:7.6:*:*:*:*:*:*:* cpe:2.3:a:vmware:vrealize_suite_lifecycle_manager:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_cloud_foundation:-:*:*:*:*:*:*:* | CWE-287 |
| CVE-2022-31658 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-94 |
| CVE-2022-31665 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-94 |
| CVE-2022-31659 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-89 |
| CVE-2022-31657 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-601 |

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2022-31660 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-264 |
| CVE-2022-31661 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-264 |
| CVE-2022-31664 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-264 |
| CVE-2022-31662 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-22 |
| CVE-2022-31663 | VMware Workspace ONE Access: 21.08.0.0 - 21.08.0.1 | cpe:2.3:a:vmware:vmware_workspace_one_access:-:*:*:*:*:*:*:* | CWE-79 |

## Patch Links

https://kb.vmware.com/s/article/89096

## References

https://www.vmware.com/security/advisories/VMSA-2022-0021.html

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.


At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**August 3, 2022 . 10:12 PM**

© 2022 All Rights are Reserved by HivePro

More at www.hivepro.com