

EXECUTIVE SUMMARY

VMware Authentication Bypass Vulnerability ([CVE-2022-22972](#)) allows attackers to log in as a local user in VMware products. The vulnerability was found by the Horizon3 team which is a penetration testing company.

VMware recently patched a critical authentication bypass vulnerability in their VMware Workspace ONE Access, Identity Manager and vRealize Automation products ([CVE-2022-22972](#)).

VMware issued a [security advisory](#) on May 18, 2022, for vulnerabilities affecting Workspace ONE Access, vRealize Automation, and VMware Identity Manager products.

Vulnerability-related PoC has been published that allows threat actors [to bypass authentication](#) across multiple [VMware products](#). VMware previously shared patches for the vulnerability.

VMware has urged customers to patch a pair of critical flaws in some of their products. The vulnerabilities allow for authentication bypass and a privilege escalation. [CVE-2022-22972](#) has been scored as 9.8 out of 10 on the CVSSv3 scale. CVE-2022-22973 has yet to be assigned a score

On April 6, 2022, VMware published a security advisory mentioning eight vulnerabilities including [CVE-2022-22972](#) which impacts their products VMware Workspace ONE Access, Identity Manager and vRealize Automation. On April 13, they updated their advisory with information that CVE-2022-22952 is being exploited in the wild.

Multiple writeups detailing exploitation scenarios for the aforementioned two vulnerabilities were published in the last week of April, finally followed by a CISA Alert on May 18. The CISA Alert also calls out [CVE-2022-22972](#) and [CVE-2022-22973](#) – published on the same day and affecting the same products – as being highly likely to be exploited.

1- Introduction:

Some VMWare products have vulnerabilities. These are ONE Access, Identity Manager, and vRealize Automation. The specific vulnerability we will examine is **VMware Authentication Bypass Vulnerability**. This vulnerability allows an attacker to log in as any known local user. The vulnerability is about authentication bypass and it's affecting local domain users. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8. VMware Authentication Bypass Vulnerability. The vulnerability was found by Bruno López and there is a write-up on this vulnerability by the Horizon3 team.



2- Explanation of the vulnerability with its impact:

A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. The tactic that has been used is Privilege escalation (TA0029) and the technique is Abuse Elevation Control Mechanism (T1548). A malicious actor may be able to obtain administrative access. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

The Impact of the Vulnerability Can Be Massive

```
dev@ubuntu:~/Downloads/server$ sudo python3 socket_server.py
[sudo] password for dev:
Got data b'POST /SAAS/API/1.0/REST/auth/local/login HTTP/1.1\r\nAccept: application/json\r\nContent-Type: application/json\r\nContent-Length: 125\r\nHost: 192.168.25.61:443\r\nConnection: Keep-Alive\r\nUser-Agent: Apache-HttpClient/4.5.3 (Java/1.8.0_201)\r\nAccept-Encoding: gzip,deflate\r\n\r\n{"organizationName": "VSPHERE.LOCAL", "username": "administrator", "password": "asdf", "isSsoToken": false, "domain": "vsphere.local"}'
dev@ubuntu:~/Downloads/server$
```

Security researchers easily accessed the system by exploiting the vulnerability.

Some Impacts: An attacker with network access can obtain administrator access. An attacker with local access can become root on the virtual appliance. Affected Products are:

- 1- VMware Workspace ONE Access (Access) ([Versions: 21.08.0.0, 21.08.0.1, 20.10.0.0, 20.10.0.1](#))
- 2- VMware Identity Manager (vIDM) ([Versions: 3.3.3, 3.3.4, 3.3.5, 3.3.6](#))
- 3- VMware vRealize Automation (vRA) ([Version: 7.6, 8.x](#))
- 4- VMware Cloud Foundation ([Versions: 4.3.x, 4.2.x, 4.1, 4.0.x, 3.x](#))
- 5- vRealize Suite Lifecycle Manager ([8.x](#))

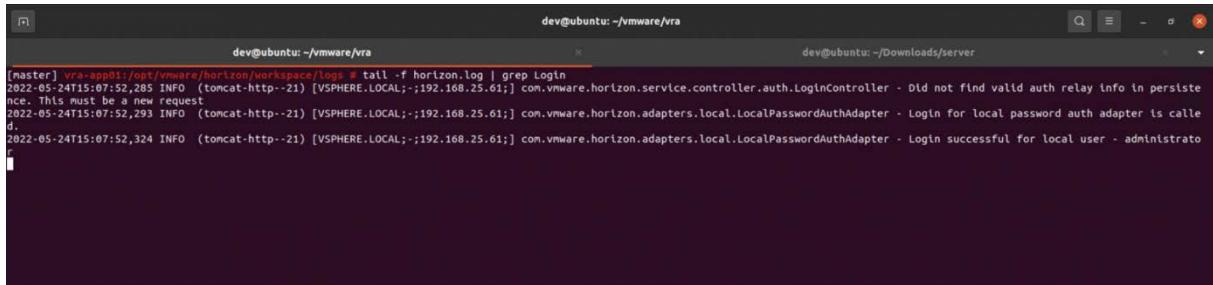
3- Explanation of the exploit:

A team called Horizon3 which enables organizations to continuously assess the security posture of their enterprise across many attack surfaces released a **proof-of-concept (PoC)** exploit.

"This script can be used by bypassing authentication on vRealize Automation 7.6 using CVE-2022-22972," the researchers said.

"Workspace ONE and vIDM have different authentication endpoints, but the crux of the vulnerability remains the same.

CVE-2022-22972 is a relatively simple 'Host' header manipulation vulnerability. Motivated attackers would not have a hard time developing an exploit for this vulnerability," Horizon3 added.



```
dev@ubuntu: ~/vmware/vra
dev@ubuntu: ~/Downloads/server

[master] vra@pphi:/opt/vmware/horizon/workspace/logs # tail -f horizon.log | grep Login
2022-05-24T15:07:52,285 INFO (tomcat-http--21) [VSPHERE.LOCAL;-;192.168.25.61;] com.vmware.horizon.service.controller.auth.LoginController - Did not find valid auth relay info in persistence. This must be a new request.
2022-05-24T15:07:52,293 INFO (tomcat-http--21) [VSPHERE.LOCAL;-;192.168.25.61;] com.vmware.horizon.adapters.local.LocalPasswordAuthAdapter - Login for local password auth adapter is called.
2022-05-24T15:07:52,324 INFO (tomcat-http--21) [VSPHERE.LOCAL;-;192.168.25.61;] com.vmware.horizon.adapters.local.LocalPasswordAuthAdapter - Login successful for local user - administrator
```

Successful login as vRealize Automation admin (Horizon3-Penetration test company)

In the review, researchers stated that authentication in **vRealize Automation 7.6** could be bypassed thanks to the script to be used by exploiting the vulnerability with the code CVE-2022-22972 and underlined that the exploit could be quite easy for attackers.

4- Current exploitation status:

When the vulnerability came to light, CISA issued an emergency directive instructing federal agencies to patch CVE-2022-22972 and CVE-2022-22973 by May 23 or remove affected instances from their network until a patch can be applied.

The products affected by CVE-2022-22972 and CVE-2022-22973 are also impacted by **CVE-2022-22954** and **CVE-2022-22960**, which have been exploited in the wild — both separately and chained — by multiple threat groups since early April.

5- Mitigation suggestions:

When the vulnerability came to light, CISA issued an emergency directive instructing federal agencies to patch CVE-2022-22972 and CVE-2022-22973 by May 23 or remove affected instances from their network until a patch can be applied.

VMware customers should patch their Workspace ONE Access, Identity Manager, and vRealize Automation installations immediately (check the list below), without waiting for a regular patch cycle to occur. VMware has instructions here on patching and applying workarounds.

Additionally, if your installation is internet-facing, consider taking steps to remove direct access from the internet.

It may also be prudent to follow CISA's guidance on post-exploitation detection methods found in Alert (AA22-138B).

Impacted Appliances

Product Component	Affected Version(s)
VMware Workspace ONE Access Appliance	21.08.0.0 21.08.0.1 20.10.0.0 20.10.0.1
VMware Identity Manager Appliance	3.3.3 3.3.4 3.3.5 3.3.6
VMware Realize Automation 7.6	7.6

6- Conclusion:

CVE-2022-22972 is a relatively simple Host header manipulation vulnerability. Motivated attackers would not have a hard time developing an exploit for this vulnerability. A quick search on Shodan.io for the affected VMware applications returns a pretty low count of organizations that expose them to the internet. Of note, the healthcare, education industry, and state government all seem to be a fair amount of the types of organizations that have exposures – putting them at larger risk for current and future exploitation. Organizations should address these issues by immediately following the guidance within the VMware Security Advisory.

A set of critical vulnerabilities that VMware patched in April started to be exploited in the wild just 48 hours after the company released an alert and the corresponding fixes, to install cryptocurrency miners and backdoors.