VMware Workspace ONE Access and Identity Manager CVE-2022-22954 Vulnerability

On April 6, 2022 VMware released VMSA-2022-0011, a critical advisory addressing security vulnerabilities found and resolved in VMware's Workspace ONE Access, VMware Identity Manager (vIDM), vRealize Lifecycle Manager, vRealize Automation, and VMware Cloud Foundation products. [1] VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution. [2] Additionally, the identifier CVE-2022-30190 has been assigned to this vulnerability. CWE number of this vulnerability : CWE-94: Improper Control of Generation of Code.

What Is the VMware Workspace ONE Access and Identity Manager CVE-2022-22954 Vulnerability

The VMware Workspace One Access (formerly VMware Identity Manager) application running on the remote host is affected by a remote code execution vulnerability due to server-side template injection. An unauthenticated, remote attacker can exploit this, via a specially crafted message, to execute arbitrary code on the remote host. In one attack, a threat actor with network access to the web interface exploited CVE 2022-22954 to execute a shell command as a VMWare user, then exploited the second flaw to escalate privileges to root. After exploiting both flaws, the threat actor could move laterally to other systems, escalate permissions, and wipe logs. In another case, a threat actor deployed the Dingo-J-spy web shell after exploiting the flaws. Exploits for the two April vulnerabilities were developed by reverse-engineering the patches released by VMWare. Now patches have been released to fix the latest two vulnerabilities, similarly rapid exploitation of the flaws in the wild can be expected..[3]

Which Products Are Affected ?

- VMware Workspace ONE Access, versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0
- vIDM versions 3.3.6, 3.3.5, 3.3.4, 3.3.3
- VMware Cloud Foundation, 4.x
- vRealize Suite LifeCycle Manager, 8.x

How attackers exploit the vulnerability ?

The attacker runs an execute command at the get parameter. He adds the whoami command to this parameter to learn the user. Then he displays the folders with the ls -la command. Finally, he can add the desired file to the desired folder on the server with the get parameter

Incident Response

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

Solution proposals

Vmware company has released a patch to close security vulnerabilities. It is recommended to update the application immediately, as this is a critical level(CVSS 9.8) of security. Due to its active exploitation, if you haven’t applied the VMware security updates or mitigations yet, it is extremely urgent to do so as soon as possible. For users of VMware products, it is worth noting that the vendor’s advisory lists several high severity flaws apart from the aforementioned RCE, which affect additional products besides Workspace One Access and Identity Manager, so make sure that you’re using the latest available version.[4]

References

[1] “VMSA-2022-0011: Questions & Answers” June 12,2022 [Online]. Available: https://core.vmware.com/vmsa-2022-0011-questions-answers-faq#section1
[2] "VMSA-2022-0011" June 12,2022 [Online]. Available: https://www.vmware.com/security/advisories/VMSA-2022-0011.html
[3] HIPAA Journal, “ CISA Issues Emergency Directive to Patch Vulnerable VMWare Products ” June 12,2022 [Online]. Available: https://www.hipaajournal.com/cisa-issues-emergency-directive-to-patch-vulnerable-vmware-products/
[4] Bill Toulas, ” Hackers exploit critical VMware CVE-2022-22954 bug, patch now ” June 12,2022 [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-vmware-cve-2022-22954-bug-patch-now/