Summary

In definition: CVE-2022-22960 is a privilege escalation vulnerability that we seen in VMware Workspace ONE Access Identity Manager and vRealize Automation instances, by the reason of improper permissions in support scripts. A malicious actor can escalate privileges as a “root” user.

Introduction

Multiple vulnerabilities in VMware were privately reported. Patches are available to fix these vulnerabilities in affected VMware products.

Explanation Of The Vulnerability And Exploit

VMware has confirmed that exploitation of CVE-2022-22960 has occurred in the wild. Attackers can, for this reason, leverage CVE-2022-22954 to remotely execute commands to overwrite specific paths. If successful, CVE-2022-22960 can then be leveraged to execute these overwritten paths with root permissions using the sudo command. Researches so far has shown us, one publicly known sample demonstrating exploitation of CVE-2022-22960 by overwriting the /usr/local/horizon/scripts/publishCaCert.hzn file.

CISA (Certified Information System Auditor) derived a notice warning to organizations of potential exploitation attempts of known vulnerabilities in the VMware products tracked as CVE-2022-22954 and CVE-2022-22960. If that vulnerabilities once exploited, the revealed flaws give green light to threat actors to perform malicious template injenction on the server end. If we need to speak more specifically, the exploitation of the CVE-2022-22954 can lead to remote code execution, while the CVE-20222-22960 flaw can be weaponized for privilege escalation. The fact is that the newly discovered VMware bugs can be a source of exploit chain attack and that is going to double the risk factor.

Even if our topic was CVE-2022-22960, the actively exploited vulnerabilities are tracked as CVE-2022-22954 and CVE-2022-22960, and they allow remote code execution and privilege escalation, respectively. They can be used together for a chain attack. They affect VMware Workspace ONE Access, Identity Manager, and vRealize Automation, and they were patched in early April.

Mitigation

As for the mitigation measures in response to CVE-2022-22954 and CVE-2022-22960 exploitation, the affected VMware products should be promptly updated to the latest version. Also, to minimize the risks of related exploit chain attacks, organizations are recommended to remove the affected software versions from their systems. To mitigate these vulnerabilities, we can patch the system or we can use web application firewalls. Although interest levels of these vulnerabilities have been stabilized. We will see low level scanning and attempts to exploit them for some time but even if exploits or scans remain steady, it is important

to take steps to protect our systems. To mitigate CVE-2022-22960, apply the patches shown in the below

Access	21.08.0.1, 21.08.0.0	Linux	CVE-2022-22960	7.8	Important	KB88099	KB88098	FAQ

1)Patching: Ideal time for patching is right now, particularly if the system is internet-facing in any way.

2)Web Application Firewall: Placing a web application firewall in front of our systems will add a defense against zero day attacks and other vulnerabilities.

Conclusion

Those type of vulnerabilities can be very harmful for our and other systems. If root user privileges fall into the hands of an unwanted user, they can read, write, copy, delete, modify files and etc. That is why we need to keep our system updated and have a web application firewall. Risk rating is shown under below.