Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

VMware could not fix a vulnerability that has been disclosed for eleven months

Date of Publication	Admiralty Code	TA Number
October 13, 2022	A1	TA2022222

Summary

VMware disclosed a vulnerability in November 2021 that has not been fixed as of October 2022. VMware initially patched this vulnerability, but later discovered that it did not fix it. The vulnerability can be exploited by an attacker to escalate to a SYSTEM.

CVE

CVE	NAME	PATCH
CVE-2021-22048	VMware vCenter Server IWA privilege escalation vulnerability	✗

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	**T1548** Abuse Elevation Control Mechanism	**T1068** Exploitation for Privilege Escalation	**TA0001** Initial Access
T1190 Exploit Public-Facing Application			

Technical Details

The vulnerability can be exploited by attackers with non-administrative access to elevate privileges. This flaw, however, can only be exploited by attackers using a vector network adjacent to the targeted server in high-complexity attacks requiring low privileges and no user interaction. While patches are pending for all affected products, VMware has provided a workaround to remove the attack vector.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2021-22048	vCenter Server: 8.0, 7.0, 6.7, 6.5	cpe:2.3:a:vmware:vcenter_server:*:-:*:*:*:*:*:*	CWE-264

References

https://www.vmware.com/security/advisories/VMSA-2021-0025.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous 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

October 13, 2022 . 12:00 AM

More at www.hivepro.com