Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Vulnerabilities in VMware when chained together grant full system control

Date of Publication

19 May 2022

TA Number

TA2022105

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning to organizations about malicious actors using CVE-2022-22954 and CVE-2022-22960. This alert was published following the disclosure of two related vulnerabilities (CVE-2022-22972 and CVE-2022-22973), rendering it vulnerable to future exploitation. All these flaws might be exploited separately or in combination to obtain total control.

CVEs

CVE	NAME	PATCH
CVE-2022-22954	Server-side Template Injection Remote Code Execution Vulnerability	✓
CVE-2022-22960	Local Privilege Escalation Vulnerability	✓
CVE-2022-22972	Authentication Bypass Vulnerability	✓
CVE-2022-22973	Local Privilege Escalation Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0011** Command and Control	**T1588** Obtain Capabilities	**T1588.006** Obtain Capabilities: Vulnerabilities
T1588.005 Obtain Capabilities: Exploits	**T1190** Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1573** Encrypted Channel
T1068 Exploitation for Privilege Escalation	**T1548** Abuse Elevation Control Mechanism	**T1221** Template Injection	

Technical Details

#1

On 6th April 2022, VMware made organizations aware of CVE-2022-22954 & CVE-2022-22960. Just 48 hours after the patch was released malicious threat actors were able to develop a new exploit by reverse engineering the patch and began exploiting vulnerable products. Rocket Kitten was one of the threat actors that were observed exploiting CVE-2022-22954.

#2

On 18th May 2022, VMware released two vulnerabilities(CVE-2022-22972 & CVE-2022-22973). Due to the vulnerabilities impacting the same products, CISA expects threat actor to develop capabilities to exploit these vulnerabilities.

#3

All the above vulnerabilities can be exploited by an attacker to trigger server-side template injection causing remote code execution (CVE-2022-22954); elevate privileges to 'root' (CVE-2022-22960 & CVE-2022-22973); and get authentication bypass (CVE-2022-22972).

#4

CISA has advised organizations to update the affected VMware products to the non-vulnerable versions by 23rd May 2022 to avoid exploitation.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-22954	VMware Workspace ONE Access versions 20.10.0.0 - 21.08.0.1; vRealize Suite Lifecycle Manager versions 8.0 - 8.4.1 Patch 2; VMware Cloud Foundation versions 4.0 - 4.3.1.1; VMware Identity Manager versions 3.3.3 - 3.3.6	cpe:2.3:a:vmware:vmware_workspace_one_access:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:vrealize_suite_lifecycle_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:identity_manager:*:*:*:*:*:*:*:*:*	CWE-94
CVE-2022-22960			CWE-269
CVE-2022-22972			CWE-287
CVE-2022-22973			CWE-264

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	136.243.75[.]136
Files	horizon.jsp jquery.jsp

Patch Links

https://www.vmware.com/security/advisories/VMSA-2022-0011.html

https://www.vmware.com/security/advisories/VMSA-2022-0014.html

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-138b

https://www.cisa.gov/emergency-directive-22-03

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

19 May 2022, 5:00 PM

More at www.hivepro.com