Hive Pro

THREAT ADVISORY

VMware addresses security flaws discovered during Tianfu Cup Pwn Contest	TA2022034

Threat Level	AMBER	Publish Date – Feb 16, 2022

VMware addressed vulnerabilities in ESXi, Workstation, Fusion, and Cloud Foundation, few months after the discovery of these bugs by participants at Tianfu Cup Pwn Contest. VMware has rated some of these vulnerabilities as important, however, chaining these issues together may result in what is effectively a critical exploit. Successfully exploiting VMware Workstation might allow attackers to perform guest-to-host escape and when combined with ESXi exploitation, it may allow them to execute code as the virtual machine's VMX process and obtain root permissions on the host machine.

A Use-after-free vulnerability in XHCI USB controller (CVE-2021-22040) and a double-fetch vulnerability in UHCI USB controller (CVE-2021-22041) were reported. Attackers with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host if isochronous USB endpoint is available.

Other noted vulnerability was ESXi settingsd unauthorized access (CVE-2021-22042) which allows an attacker with privileges within the VMX process only to access settingsd service running as a high privileged user. In addition to these bugs, an ESXi settingsd TOCTOU vulnerability (CVE-2021-22043) also allows an attacker with access to settingsd to escalate their privileges by writing arbitrary files.

Organizations should apply all the patches as given below. VMware has also included workarounds in their advisories, suggesting customers that removing USB controllers from virtual machines may help resolve these issues.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0040: Impact
TA0007: Discovery
TA0004: Privilege Escalation
TA0005: Defense Evasion
T1068: Exploitation for Privilege Escalation
T1497: Virtualization/Sandbox Evasion
T1195: Supply Chain Compromise
T1499: Endpoint Denial of Service
T1499.001: Endpoint Denial of Service: Service Exhaustion Flood

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-22040	Cloud Foundation (ESXi) versions 4.x, 3.x, ESXi versions 7.0 U3, 7.0 U2, 7.0 U1, 6.7, 6.5, Fusion version 12.x, Workstation version 16.x	cpe:2.3:a:vmware:vmware_cloud_foundation:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:vmware_fusion:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:* , cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:*	Use-after-free vulnerability in XHCI USB controller	CWE-416
CVE-2021-22041			Double-fetch vulnerability in UHCI USB controller	CWE-362
CVE-2021-22042	Cloud Foundation (ESXi) versions 4.x, 3.x, ESXi versions 7.0 U3, 7.0 U2, 7.0 U1, 6.7, 6.5	cpe:2.3:a:vmware:vmware_cloud_foundation:*:*:*:*:*:*:*:*, cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:*	ESXi settingsd unauthorized access vulnerability	CWE-284
CVE-2021-22043			ESXi settingsd TOCTOU vulnerability	CWE-367
CVE-2021-22050	ESXi versions 7.0, 6.7, 6.5	cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:*	ESXi slow HTTP POST denial of service vulnerability	CWE-399

Patch Link

https://www.vmware.com/security/advisories/VMSA-2022-0004.html

References

https://www.securityweek.com/vmware-patches-vulnerabilities-reported-researchers-chinese-government
https://www.zdnet.com/article/vmware-patches-released-after-vulnerabilities-found-during-tianfu-cup/