Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical VMware Vulnerabilities Leading To Sandbox Escape

Date of Publication	Admiralty Code	TA Number
March 8, 2024	A1	TA2024094

Summary

First Seen: March 2024
Affected Products: VMware ESXi, VMware Workstation Pro / Player (Workstation), VMware Fusion Pro / Fusion (Fusion), VMware Cloud Foundation (Cloud Foundation)
Impact: Critical vulnerabilities tracked as CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255 have been addressed by Vmware. These vulnerabilities allow attackers to bypass virtual machines and execute commands on the host machine. Workstation, Fusion, Cloud Foundation, and VMware ESXi are all impacted by these vulnerabilities.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-22252 Critical	VMware Use-after-free Vulnerability	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation (Cloud Foundation)	✗	✗	✓
CVE-2024-22253 Critical	VMware Use-after-free Vulnerability		✗	✗	✓
CVE-2024-22254	VMware ESXi Out-of-bounds write Vulnerability		✗	✗	✓
CVE-2024-22255	VMware Information disclosure vulnerability		✗	✗	✓

Vulnerability Details

#1 VMware has addressed numerous vulnerabilities in VMware ESXi, Workstation, and Fusion, including CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. These vulnerabilities could potentially allow attackers to circumvent hypervisor and sandbox security measures across all affected versions.

#2 The CVE-2024-22252 vulnerability stems from a use-after-free issue in the XHCI USB controller, while CVE-2024-22253 arises from a similar problem in the UHCI USB controller. These vulnerabilities could enable a remote attacker with administrative access to the guest operating system to execute arbitrary code on the host operating system, triggering a use-after-free error. In the context of Workstation and Fusion, this could lead to code execution on the host system where these applications are installed. However, in the case of ESXi, the exploitation is confined within the VMX sandbox.

#3 Processing unknown input might lead to a boundary error, which is the source of the CVE-2024-22254 vulnerability. This vulnerability could be used by an attacker with VMX process capabilities to execute command and leading to an escape of the sandbox. Regarding CVE-2024-22255, the UHCI USB controller's excessive data output is the source of the vulnerability. It is possible for a remote user to read private information from the memory of the VMX process if they have administrative access to the guest operating system.

#4 In response to the vulnerabilities, VMware has also provided a **workaround**, which is to remove USB controllers from virtual machines. Administrators are advised to consider the repercussions before implementing the workarounds. Although no active exploitation of the vulnerabilities has been discovered as of yet, administrators are strongly advised to patch their systems with the most recent versions in order to prevent future exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-22252	Vmware ESXi- Before ESXi80U2sb-23305545 VMware Fusion: 13.x - 13.5 VMware Workstation: 17.x - 17.5	cpe:2.3:a:vmware:esxi:*:*:*:*:*:*:* cpe:2.3:a:vmware:Fusion:*:*:*:*:*:*:* cpe:2.3:a:vmware:Workstation:*:*:*:*:*:*:*	CWE-416
CVE-2024-22253			CWE-416
CVE-2024-22254			CWE-787
CVE-2024-22255			CWE-200

Recommendations

Apply Patch: Install the security patch provided by VMware to address the CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Least Privilege: Adhere to the idea of "least privilege" by giving users/ application only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1497 Virtualization/Sandbox Evasion	T1211 Exploitation for Defense Evasion

Patch Details

VMware has released patches for these vulnerabilities in the latest versions,
For Vmware Workstation upgrade to version- 17.5.1
For Vmware Fusion upgrade to version- 13.5.1
For Vmware ESXi upgrade to the version- ESXi80U1d-23299997

Link:
https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-80u2b-release-notes/index.html
https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-80u1d-release-notes/index.html
https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u3p-release-notes/index.html

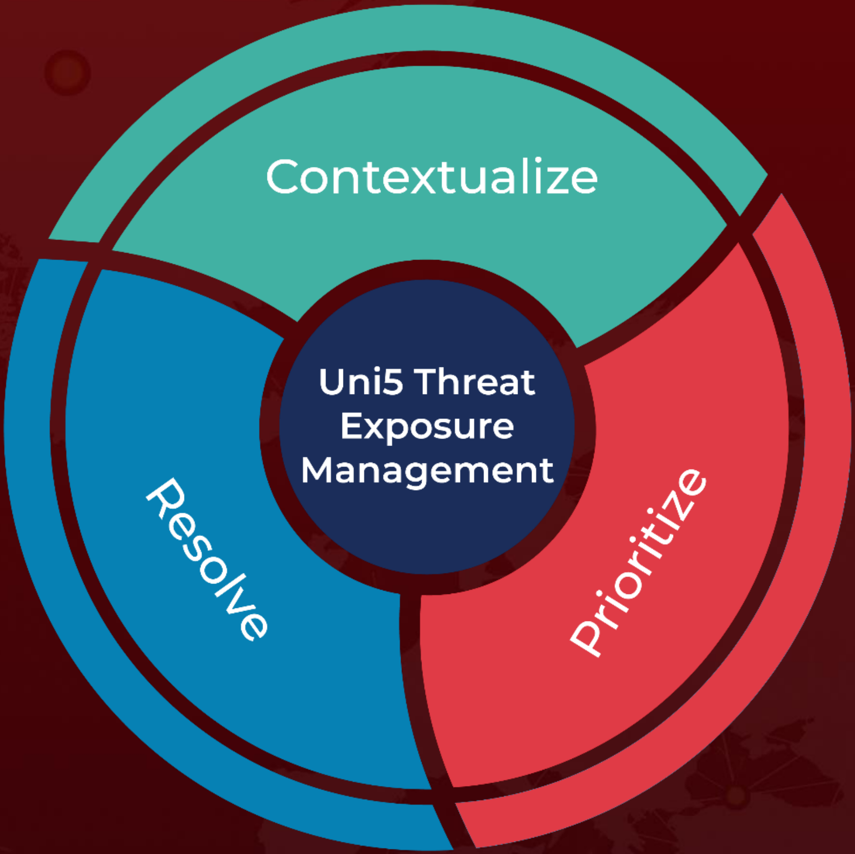
References

https://www.vmware.com/security/advisories/VMSA-2024-0006.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 8, 2024 • 6:00 AM

More at www.hivepro.com