Security Advisory 2022-013

Multiple Vulnerabilities in VMware

February 17, 2022 — v1.0

TLP:WHITE

History:

- *17/02/2022 — v1.0 – Initial publication*

Summary

On January 15th, VMware released several security patches for high-severity flaws affecting multiple products. The vulnerabilities identified as `CVE-2021-22040`, `CVE-2021-22041`, `CVE-2021-22042`, `CVE-2021-22043`, `CVE-2021-22050`, `CVE-2022-22945` can lead to multiple effects such as arbitrary code execution, denial of service, and privilege escalation.

There is no evidence that any of the weaknesses are exploited in the wild. However, it is recommended to patch as soon as possible [1].

Technical Details

Here are the technical details of these vulnerabilities :

- `CVE-2021-22040` - CVSS score: 8.4 - is a use-after-free vulnerability in XHCI USB controller. A malicious actor 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.
- `CVE-2021-22041` - CVSS score: 8.4 - is a double-fetch vulnerability in UHCI USB controller. A malicious actor 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.
- `CVE-2021-22042` - CVSS score: 8.2 - is a ESXi `settingsd` unauthorised access vulnerability. A malicious actor with privileges within the VMX process only, may be able to access `settingsd` service running as a high privileged user.
- `CVE-2021-22043` - CVSS score: 8.2 - is a ESXi `settingsd` TOCTOU vulnerability. A malicious actor with network access to ESXi may exploit this issue to create a denial-of-service condition by overwhelming `rhttpproxy` service with multiple requests.
- `CVE-2021-22050` - CVSS score: 5.3 - is a ESXi slow HTTP POST denial-of-service vulnerability. A malicious actor with network access to ESXi may exploit this issue to create a denial-of-service condition by overwhelming `rhttpproxy` service with multiple requests.
- `CVE-2022-22945` - CVSS score: 8.8 - is a CLI shell injection vulnerability in the NSX Edge appliance component. A malicious actor with SSH access to an NSX-Edge appliance (NSX-V) can execute arbitrary commands on the operating system as root.

Affected Products

- VMware ESXi versions 7.0 U3 before ESXi70U3c-19193900
- VMware ESXi versions 7.0 U2 before ESXi70U2e-19290878
- VMware ESXi versions 7.0 U1 before ESXi70U1e-19324898
- VMware ESXi versions 6.7 before ESXi670-202111101-SG
- VMware ESXi versions 6.5 before ESXi650-202202401-SG or ESXi650-202110101-SG
- VMware Fusion versions 12.x before 12.2.1
- VMware Workstation versions 16.x before 16.2.1
- NSX Data Center for vSphere versions before 6.4.13

Recommendations

Please refer to the security advisories from the editor to get security patches [2, 3].

References

[1] https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html

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

[3] https://www.vmware.com/security/advisories/VMSA-2022-0005.html