Security Advisory 2024-024

Vulnerabilities in VMware Products

March 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/03/2024 — v1.0 – Initial publication*

Summary

On March 5, 2024, VMware released fixes for four vulnerabilities affecting several VMware products. The most serious bugs could allow a malicious actor with local admin privileges on a virtual machine to execute code as the virtual machine's VMX process running on the host.

It is recommended upgrading affected software as soon as possible.

Technical Details

The vulnerabilities **CVE-2024-22252** and **CVE-2024-22253**, both with a CVSS score of 9.3 Workstation/Fusion and of 8.4 for ESXi, are Use-after-free vulnerability in XHCI USB controller and in the 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. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.

The vulnerability **CVE-2024-22254**, with a CVSS score of 7.9, is an out-of-bounds write vulnerability in ESXi. A malicious actor with privileges within the VMX process may trigger an out-of-bounds write leading to an escape of the sandbox.

The vulnerability **CVE-2024-22255**, with a CVSS score of 7.1, is an information disclosure vulnerability in the UHCI USB controller. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process.

Affected Products

These vulnerabilities affect VMware ESXi 7.0 and 8.0, VMware Workstation 17.x and VMware Fusion 13.x.

Recommendations

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor [1].

References

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