SecurityRisk ADVISORS

Threat Intelligence Gathering & Research Team

TB22-1214-Yellow-VMware

December 14, 2022

EXECUTIVE SUMMARY

VMware released two security advisories notifying customers of three newly identified vulnerabilities affecting several VMware products. The advisories include details on CVE-2022-31702, CVE-2022-31703, and CVE-2022-31705. While the vulnerabilities have been added to CISA's National Vulnerability Database, analysts have not yet confirmed CVSSv3 severity scores for any of the vulnerabilities. VMware estimates the severity of the three vulnerabilities to be between 5.9 and 9.8.

DESCRIPTION

CVE-2022-31702 is a command injection vulnerability in VMware's vRealize Network Insight's REST API. The vulnerability requires a malicious actor to have previous network access to execute commands without authentication. VMware's vRealize Network Insight's REST API also includes CVE-2022-31703, a directory traversal vulnerability. Similarly, an adversary could read arbitrary files from the server if they have network access.

CVE-2022-31705 is an out-of-bounds write vulnerability in the USB 2.0 controller of VMware's ESXi, Workstation, and Fusion products. A threat actor with local administrative privileges on a virtual machine could exploit this vulnerability to execute code on the host machine.

AFFECTED PRODUCTS

The following products are impacted by CVE-2022-31705.

- VMware ESXi
- VMware Workstation Pro / Player
- VMware Fusion Pro / Fusion
- VMware Cloud Foundation

The following product is impacted by CVE-2022-31702 and CVE-2022-31703.

- VMware vRealize Network Insight (vRNI)

SAFEGUARDS/RECOMMENDATIONS

VMware includes a Response Matrix in its security advisories with the necessary patches needed for each vulnerability and their corresponding affected products.

- ESXi 8.0 users should upgrade to version 8.0a to ensure necessary patches are made.
- ESXi 7.0 users should upgrade to version 7.0 Update 3i.
- Fusion 12.x users running on OS X should update systems to version 12.2.5.
- Workstation users running version 16.x should update to version 16.2.5.
- vRNI users running versions 6.2-6.8.0 should upgrade to versions 6.2 HF-6.8.0 HF, respectively.

REFERENCES

- https://www.cisa.gov/uscert/ncas/current-activity/2022/12/13/vmware-releases-security-updates-multiple-products
- https://www.vmware.com/security/advisories/VMSA-2022-0031.html#
- https://www.vmware.com/security/advisories/VMSA-2022-0033.html

Version History

Version 1. Initial Report