Hackers Exploiting New VMware Zero-Day Since October 2024 - InfoSecBu

Data: 2025-09-30 18:31:37

Autor: Inteligência Against Invaders

A newly patched security flaw in Broadcom VMware Tools and VMware Aria Operations has been ***exploited*** by a threat actor named UNC5174 since mid-October 2024, according to NVISO Labs.

The vulnerability identified as CVE-2025-41244 (CVSS score: 7.8) is a flaw that allows local privilege escalation, impacting the following versions –

VMware Cloud Foundation 4.x and 5.x
VMware Cloud Foundation 9.x.x.x
VMware Cloud Foundation 13.x.x.x (Windows, Linux)
VMware vSphere Foundation 9.x.x.x
VMware vSphere Foundation 13.x.x.x (Windows, Linux)
VMware Aria Operations 8.x
VMware Tools 11.x.x, 12.x.x, and 13.x.x (Windows, Linux)
VMware Telco Cloud Platform 4.x and 5.x
VMware Telco Cloud Infrastructure 2.x and 3.x

“A malicious local actor with non-administrative privileges having access to a VM with VMware Tools installed and managed by Aria Operations with SDMP enabled may exploit this vulnerability to escalate privileges to root on the same VM,” VMware said in an advisory released Monday.

Local privilege escalation means the attacker must gain access to the infected device in another way.

Maxime Thiebaut from NVISO discovered a flaw on May 19, 2025, during an incident response. VMware Tools version 12.4.9, included in 12.5.4, fixes the issue for Windows 32-bit systems. Linux vendors will also provide an open-vm-tools version that addresses CVE-2025-41244.

Broadcom hasn’t confirmed any real-world exploitation, but NVISO Labs linked the activity to a China-associated group called UNC5174, tracked by Google Mandiant. This group is known for exploiting security vulnerabilities in Ivanti and SAP NetWeaver for initial access.

“When successful, exploitation of the local privilege escalation results in unprivileged users achieving code execution in privileged contexts (e.g., root),” Thiebaut said. “We can however not assess whether this exploit was part of UNC5174’s capabilities or whether the zero-day’s usage was merely accidental due to its trivialness.”

The vulnerability comes from a function called “get_version()” that uses a regular expression to check if a process with a listening socket matches a certain pattern, then it runs the version command for that service.

“While this functionality works as expected for system binaries (e.g., /usr/bin/httpd), the usage of the

broad?matching S character class (matching non?whitespace characters) in several of the regex patterns also matches non-system binaries (e.g., /tmp/httpd),” Thiebaut explained. “These non-system binaries are located within directories (e.g., /tmp) which are writable to unprivileged users by design.”

This vulnerability allows a local attacker to exploit a malicious binary at “/tmp/httpd,” leading to privilege escalation when the VMware metrics service runs. The attacker just needs the binary to be executed by an unprivileged user and to open a random listening socket.

A Brussels cybersecurity firm reported that UNC5174 used “/tmp/httpd” to store a malicious file, gaining elevated root access and executing code. The specifics of the payload executed are currently unknown.

“The broad practice of mimicking system binaries (e.g., httpd) highlights the real possibility that several other malware strains have accidentally been benefiting from unintended privilege escalations for years,” Thiebaut said.