THREAT BULLETINS

Exploitation Confirmed for VMware Flaw CVE-2025-41244

TLP:WHITE

Oct 01, 2025

On September 29, 2025, Broadcom issued an advisory for a local privilege escalation flaw tracked as CVE-2025-41244, affecting VMware Tools and VMware Aria Operations guest service discovery features. According to security researchers from NVISO, the company failed to disclose active exploitation of this flaw.

Cybersecurity researchers have confirmed that a sophisticated, Chinese state-sponsored threat actor identified as UNC5174 has been covertly leveraging this flaw since at least mid-October 2024.

The successful exploitation of this vulnerability grants attackers root-level access on a virtual machine (VM) from a non-administrative account, posing an extreme risk to enterprise hybrid-cloud environments.

An attacker can exploit this by staging a malicious binary in one of these unprivileged, broadly matched paths, like /tmp/httpd, resulting in privilege escalation during the VMware metrics collection service.

This privilege escalation impacts both the older credential-based service discovery mode and the modern credential-less service discovery mode.

NVISO confidently attributed the exploitation campaign to UNC5174, a Chinese state-sponsored threat actor known for leveraging public-facing vulnerabilities for initial access. Given the exploit's trivial nature, where an actor mimics system binaries, analysts cannot definitively determine whether UNC5174 developed the zero-day themselves or discovered it during another campaign. It is also possible that other malware may have accidentally leveraged this vulnerability for years.

Reference(s)	securityweek, nviso, securityaffairs, socradar, thehackernews

Sources

https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/

https://www.securityweek.com/broadcom-fails-to-disclose-zero-day-exploitation-of-vmware-vulnerability/

https://socradar.io/vmware-cve-2025-41244-exploited/

https://securityaffairs.com/182816/uncategorized/broadcom-patches-vmware-zero-day-actively-exploited-by-unc5174.html

https://thehackernews.com/2025/09/urgent-china-linked-hackers-exploit-new.html

Recommendations

- Security teams with vulnerable VMWare instances are advised to apply patches issued by Broadcom immediately.
- Verify whether Service Discovery Management Pack (SDMP) is enabled and restrict non-administrative user permissions on affected VMs.
- Review systems for Indicators of Compromise (IoCs) associated with UNC5174 to identify potential pre-patch compromises.
- Implement stringent monitoring for suspicious process activity and listening sockets, particularly within temporary directories.

Incident Date
Sep 30, 2025 (UTC)

Alert ID 7571b6bb

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-41244, VMware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**