CVE-2025-22230

AUTHENTICATION BYPASS IN VMWARE TOOLS

Vairav CVE Report

Date: March 26, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Broadcom has disclosed a critical security vulnerability, CVE-2025-22230, affecting VMware Tools for Windows. This authentication bypass flaw allows attackers with non-administrative privileges on a Windows guest virtual machine (VM) to perform unauthorized high-privilege operations. Given its potential impact, organizations must immediately mitigate the risk.

VULNERABILITY DETAILS

CVE-2025-22230: Authentication Bypass in VMware Tools for Windows

Description: VMware Tools for Windows contains an authentication bypass vulnerability due to improper access control, allowing unauthorized privilege escalation within affected VMs.

Impact: Unauthorized privilege escalation, potential system takeover.

CVSS Score: 7.8 (High)

AFFECTED VERSIONS

- VMware Tools 11.x.x and 12.x.x

EXPLOIT DETAILS

Attackers with low privileges can exploit this flaw by bypassing authentication mechanisms and escalating their privileges within the Windows guest VM. Exploitation may lead to full system compromise, allowing adversaries to execute arbitrary commands or manipulate system configurations. No known active exploitation has been reported, but threat actors could weaponize this vulnerability if unpatched.

RECOMMENDED ACTIONS

Patch & Upgrade:

- VMware has released VMware Tools version 12.5.1, which addresses this vulnerability. All affected users should upgrade immediately.

ADDITIONAL SECURITY MEASURES

- No known workarounds exist; patching is the only effective mitigation.

- Limit access to Windows guest VMs to trusted users.
- Regularly monitor VM activity for any unauthorized privilege escalation attempts.

REFERENCES

https://securityonline.info/vmware-tools-for-windows-hit-by-cve-2025-22230-auth-bypass-flaw/

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518

https://cybersecuritynews.com/vmware-tools-for-windows-vulnerability/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com