An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2503050127

NCSC Advisory

Actively Exploited Vulnerabilities in VMware ESX Products

5th, March 2025

STATUS: TLP:CLEAR

Description

CVE ID and CVSS Score:

- CVE-2025-22224 (CVSS: 9.3)
- CVE-2025-22225 (CVSS: 8.2)
- CVE-2025-22226 (CVSS: 7.1)

Published: 2025-03-04

Vendor: VMWare

Products: VMware Telco Cloud Platform, VMware ESXi, VMware Workstation Pro / Player (Workstation), VMware Telco Cloud Infrastructure, VMware Cloud Foundation

Products affected

Product	Version
VMware ESXi	8
VMware ESXi	8
VMware Workstation	17.x
VMware Fusion	13.x
VMware Cloud Foundation	5.x
VMware Cloud Foundation	4.5.x
VMware Telco Cloud Platform	5.x, 4.x, 3.x, 2.x
VMware Telco Cloud Infrastructure	3.x, 2.x

Impact

CVE-2025-22224: VMCI heap-overflow vulnerability

Description:

VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3.

CVE-2025-22225: VMware ESXi arbitrary write vulnerability

Description:

VMware ESXi contains an arbitrary write vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.2.

CVE-2025-22226: HGFS information-disclosure vulnerability

Description:

VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.1.

Common Weakness Enumeration (CWE)[1]:

CWE-125: Out-of-bounds Read

CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition.

CWE-123: Write-what-where Condition

[1] https://cwe.mitre.org

Known Exploited Vulnerability (KEV) catalog[2]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from.

- https://nvd.nist.gov/vuln/detail/CVE-2025-22224
- https://nvd.nist.gov/vuln/detail/CVE-2025-22225
- https://nvd.nist.gov/vuln/detail/CVE-2025-22226
- https://www.cve.org/CVERecord?id=CVE-2025-22224
- https://www.cve.org/CVERecord?id=CVE-2025-22225
- https://www.cve.org/CVERecord?id=CVE-2025-22226
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog