An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611270261

NCSC Advisory

Multiple Vulnerabilities in VMware: Avi Load Balancer, Cloud Foundation, Fusion, Telco Cloud Infrastructure, Telco Cloud Platform, vCenter Server, vSphere ESXi, vSphere Foundation and VMware Workstation

27th November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

CVE-2026-123903

Published: 26th November 2026

CVSS Score[1]: 9.8

EPSS[2]: 0.61%

Products Affected

Product	Version
VMware vCenter Server	View affected versions
VMware Cloud Foundation	View affected versions
VMware Telco Cloud Platform	View affected versions
VMware Telco Cloud Infrastructure	View affected versions

Impact

VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service.

Common Weakness Enumeration[3]: CWE-287 Improper Authentication

[1] https://www.first.org/cvss/
[2] https://www.first.org/epss/
[3] https://cwe.mitre.org/

CVE-2026-123910

Published: 26th November 2026

CVSS Score[1]: 9.8

EPSS[2]: 0.39%

Products Affected

Product	Version
VMware ESX	View affected versions
VMware Cloud Foundation	View affected versions
VMware Telco Cloud Platform	View affected versions

Impact

ESX contains a heap out-of-bounds write vulnerability in the I/O filter service.

Common Weakness Enumeration[3]: CWE-787 Out-of-bounds Write

CVE-2026-123911

Published: 26th November 2026

CVSS Score[1]: 9.8

EPSS[2]: 0.36%

Products Affected

Product	Version
VMware ESX	View affected versions
VMware Cloud Foundation	View affected versions
VMware Telco Cloud Platform	View affected versions

Impact

ESX contains a use-after-free vulnerability in the I/O filter service.

Common Weakness Enumeration[3]: CWE-416 Use After Free

CVE-2026-123912

Published: 26th November 2026

CVSS Score[1]: 9.3

EPSS[2]: 0.36%

Products Affected

Product	Version
VMware ESX	View affected versions
VMware Cloud Foundation	View affected versions
VMware Telco Cloud Platform	View affected versions
VMware Workstation	View affected versions
VMware Fusion	View affected versions

Impact

VMware ESXi, Workstation, and Fusion contain an out-of-bounds write vulnerability in the XHCI USB controller.

Common Weakness Enumeration[3]: CWE-787 Out-of-bounds Write

Rialtas na hÉireann
Government of Ireland

CVE-2026-123913

Published: 26th November 2026

CVSS Score[1]: 8.2

EPSS[2]: 0.31%

Products Affected

Product	Version
VMware ESX	View affected versions
VMware Cloud Foundation	View affected versions
VMware Telco Cloud Platform	View affected versions

Impact

VMware ESX contains a stack-based buffer-overflow vulnerability in the VMkernel.

Common Weakness Enumeration[3]: CWE-121 Stack-based Buffer Overflow

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 VMware.

Full details for these and other vulnerabilities affecting Broadcom products, and the relavant updates can be found at the following link:

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39626