National Cyber Security Centre

2406280162-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in VMware ESXi, vCenter Server, VMware Cloud Foundation (CVE-2024-37085, CVE-2024-37086, CVE-2024-37087)

Friday 28th June, 2024

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.

Description

Published: 2024-06-28T09:30:00
Vendor: Broadcom VMware
Product: VMware ESXi, vCenter Server, VMware Cloud Foundation
CVE IDs:

- CVE-2024-37085 (CVSS:3.1 6.8)
- CVE-2024-37086 (CVSS:3.1 6.8)
- CVE-2024-37087 (CVSS:3.1 5.3)

CVSS3.0 Score[1]**:** 5.3-6.8

- CVE-2024-37085 (0.090890000)
- CVE-2024-37086 (0.090890000)
- CVE-2024-37087 (0.289620000)

Summary: VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management (https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html) by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.

Products Affected

- VMware ESXi
- VMware vCenter Server
- VMware Cloud Foundation

Impact

Common Weakness Enumeration (CWE)[2]**:** Authentication bypass vulnerability
Present in CISA Known Exploited Vulnerability(KEV)[3] **catalog:** NO
Used by Ransomware Operators: Not Known

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from VMware.

Additional recommendations and mitigations for listed CVEs can be found in the respective link(s) below: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre