National Cyber Security Centre

2409190171-NCSC

**Department of the Environment, Climate & Communications**

# NCSC Alert

## Critical Vulnerability exists in VMware Cloud Foundation & VMware vCenter Server

(CVE-2024-38812, CVSSv3: 9.8)
(CVE-2024-38813, CVSSv3: 7.5)

Friday 20th September, 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:** 17 September 2024
**Vendor:** Broadcom
**Product:** VMware vCenter Server, VMware Cloud Foundation
**CVE ID's:**

- CVE-2024-38812 | CVSS3.x Score[1]: 9.8 | EPSS[2]: 0.096410000;
- CVE-2024-38813 | CVSS3.x Score: 7.5 | EPSS: 0.096410000;

For up to date EPSS score, click here:

- https://api.first.org/data/v1/epss?cve=CVE-2024-38812
- https://api.first.org/data/v1/epss?cve=CVE-2024-38813

## Products Affected

- VMware vCenter Server 8.0 upto Version 8.0 Update 3a
- VMware vCenter Server 7.0 upto Version 7.0 Update 3r
- VMware Cloud Foundation 5.x
- VMware Cloud Foundation 4.x

## Impact

- **CVE-2024-38812**
  - **Common Weakness Enumeration (CWE)[3]: CWE-122 Heap-based Buffer Overflow**
    A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc().
  - **Present in CISA Known Exploited Vulnerability(KEV)[4] catalog:** NO
  - **Used by Ransomware Operators:** Not Known.

- **CVE-2024-38813**
  - **Common Weakness Enumeration (CWE):**
    - **CWE-250 Execution with Unnecessary Privileges**
      The product performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses.
    - **CWE-273** Improper Check for Dropped Privileges:
      The product attempts to drop privileges but does not check or incorrectly checks to see if the drop succeeded.
  - **Present in CISA Known Exploited Vulnerability(KEV) catalog:** NO
  - **Used by Ransomware Operators:** Not Known.

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] 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 Broadcom.

Additional recommendations and mitigation's for CVE-2024-38812 and CVE-2024-38813 can be found in the link below:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

**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 K7X4,
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