National Cyber Security Centre

2406180171-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Heap-Overflow and Privilege Escalation Vulnerabilities in VMware vCenter Server

Wednesday 19th 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-Jun-18
Vendor: Broadcom
Products: VMware vCenter Server and VMware Cloud Foundation
CVE IDs:

- CVE-2024-37079 (CVSS:3.1 9.8)
- CVE-2024-37080 (CVSS:3.1 9.8)
- CVE-2024-37081 (CVSS:3.1 7.8)

Summary: Multiple heap-overflow and privilege escalation vulnerabilities in vCenter Server

More information related to this issue can be found at the following link:
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453

Products Affected

VMware vCenter Server multiple heap-overflow vulnerabilities (CVE-2024-37079, CVE-2024-37080)

- The vCenter Server contains multiple heap-overflow vulnerabilities in the implementation of the DCERPC protocol. VMware has evaluated the severity of these issues to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

VMware vCenter multiple local privilege escalation vulnerabilities (CVE-2024-37081)

- The vCenter Server contains multiple local privilege escalation vulnerabilities due to misconfiguration of sudo. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.8.

Recommendations

The NCSC strongly advises organisations to review the Broadcom advisory (https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24453) and apply available updates as soon as possible.

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