National Cyber Security Centre

26102201000-NCSC

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

NCSC Alert

Critical Vulnerabilities in VMware Cloud Foundation Platform CVE-2021-39144

26 October 2022

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

VMware has released a software update that addresses CVE-2021-39144, a critical vulnerability in the VMware Cloud Foundation platform. The vulnerability is in the XStream open-source library that is used by VMware Cloud Foundation.

CVE-2021-39144 is a critical vulnerability with a CVSSv3 base score of **9.8**. Exploitation of this vulnerability could enable an attacker to perform remote code execution with root-level privileges.

There is currently no known PoC and there have been no reports, as of yet, of this vulnerability being exploited in the wild.

Products Affected

All versions of VMware NSX Data Center for vSphere (NSX-V) prior to NSX-V 6.4.14 appliances.

Impact

Remote code execution, denial of service, access to sensitive data.

Recommendations

The NCSC strongly advises affected organisations to apply the KB 89809 patch released by VMware on 25 October 2022. More information can be found here: https://kb.vmware.com/s/article/89809

The above patch also addresses CVE-2022-31678. This vulnerability has a CVSSv3 score of 5.3 and exploitation could lead to denial of service or information disclosure following successful XML external entity injection (XXE) attacks.

This patch will remediate both vulnerabilities.

For organisations that are unable to apply the patch immediately, VMware have also released details of a workaround as a temporary mitigation measure, details of which can be found here: https://kb.vmware.com/s/article/89809

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
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie