National Cyber Security Centre

2102251000-NCSC

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

NCSC Flash Alert

Unauthorised RCE in VMware vCenter & ESXi
2021-02-25

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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.*

Threat Type	VMware have released a security advisory that addresses multiple vulnerabilities which include a critical (CVSS score of 9.8) Remote Code Execution (RCE) vulnerability in their vCenter Server management platform. The vulnerabilities, if exploited, could allow a threat actor to potentially take control of affected systems. There are updates available that will remedy these vulnerabilities. • **CVE-2021-21972 (CVSS Score:Base 9.8):** A Remote Code Execution vulnerability in the vSphere Client, can be exploited remotely by unauthenticated attackers in low complexity attacks that do not require user interaction. The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin that allows an attacker with network access to port 443 could execute commands with unrestricted privileges on the operating system that hosts vCenter Server. • **CVE-2021-21974 (CVSS Score: Base 8.8):** An ESXi OpenSLP heap-overflow vulnerability. OpenSLP as used in ESXi has a heap-overflow vulnerability that could enable malicious attackers inhabiting the same network segment as ESXi and with access to port 427 to execute arbitrary code remotely on impacted devices.
Products Affected	• **CVE-2021-21972** - vCenter Server 6.5, 6.7, 7.0 Impacted Product Suites that Deploy Response Matrix 3a Components: - Cloud Foundation (vCenter Server) 3.x and 4.x • **CVE-2021-21974** - ESXi 6.5, 6.7, 7.0 Impacted Product Suites that Deploy Response Matrix 3a Components: - Cloud Foundation (vCenter Server) 3.x and 4.x
Impact	Remote Code Execution
Recommendations	NCSC-IE recommends the following action: • Please install the patches supplied by VMware as quickly as possible. Security patches and workarounds can be found here. As an PoC is now available, the NCSC recommends affected parties **patch or implement the workarounds as soon as possible**. • **CVE-2021-21974** - VMware have released a guideline with steps to consume ESXi hot patch asynchronously on top of latest VMware Cloud Foundation (VCF) supported ESXi build.

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