NCSC
National Cyber Security Centre

2105261026-NCSC

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

NCSC Alert

VMware vCenter Server RCE & Authentication Vulnerabilities (CVE-2021-21985, CVE-2021-21986) 2021-05-26

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 has issued an advisory in relation to multiple vulnerabilities that exist in the vSphere Client (HTML5). The full advisory can be found here. • **(CVE-2021-21985)**: The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. (CVSS: 3.11 Base Score: 9.8 - Critical) • **(CVE-2021-21986)**: The vSphere Client (HTML5) contains a vulnerability in a vSphere authentication mechanism for the Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, and VMware Cloud Director Availability plug-ins. (CVSS: 3.11 Base Score: 6.5 - Moderate)
Products Affected	• VMware vCenter Server (vCenter Server) • VMware Cloud Foundation (Cloud Foundation)
Impact	• **CVE-2021-21985**: – A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. • **CVE-2021-21986**: – A malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication.
Recommendations	The NCSC recommends that affected organisations review the guidance and advice provided by VMware and to apply the relevant patches described in that document. Workarounds are also listed in the VMware advisory.

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