National Cyber Security Centre

2109220831-NCSC

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

NCSC Alert

VMware vCenter Server Security Vulnerabilities
2021-09-22

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.*

Description

Multiple vulnerabilities in VMware vCenter Server have been privately reported to VMware. Updates are available to remediate these vulnerabilities in affected VMware products. Included on the list of vulnerabilities is a critical advisory that requires immediate attention:

- **vCenter Server file upload vulnerability (CVE-2021-22005)**
  - The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8. More information on this vulnerability can be found here.

The full list of vulnerabilities can be found here.

Products Affected

vCenter Server 6.5, 6.7, and 7.0.

Impact

Remote Code Execution - compromised systems, data loss.

Recommendations

The NCSC recommends that affected organisations review the VMWare Advisory and follow the recommended steps to protect yourself:

- Check the VMSA to ensure you are running an affected version of vCenter Server. Organizations that updated to vCenter Server 7.0 Update 2c, for instance, may not be vulnerable to the critical vulnerability.
- If possible patch vCenter Server as soon as possible.
  - If you cannot patch right away there are workarounds linked from the VMSA for the critical vulnerability. This involves editing a text file on the VCSA and restarting services and is documented as part of the VMSA advisory here.
- You may have other security controls in your environment that can help protect you until you are able to patch. Using network perimeter access controls or the vCenter Server Appliance firewall to curtail access to the vCenter Server management interfaces, for example. VMware suggest limiting access to vCenter Server, ESXi, and vSphere management interfaces to only vSphere Admins.
- Disabling the Customer Experience Improvement Program (CEIP) will not be effective in preventing exploitation of vulnerabilities in the CEIP (analytics) service. Customers should review KB85717 to implement an effective (but temporary) workaround to prevent exploitation of known vulnerabilities in the CEIP service without functionality impact.

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