National Cyber Security Centre

2012091357-NCSC

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

NCSC Flash Alert

Command Injection Vulnerability in VMware products

2020-12-09

https://www.ncsc.gov.ie/

certreport@decc.gov.ie

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	The NCSC has received information that advanced threat actors are actively exploiting vulnerabilities that exist in VMware products. CVE-2020-4006 relates to a Command Injection Vulnerability in VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector administrative configurator. A malicious actor with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges on the underlying operating system.
Products Affected	These vulnerabilities affect the following VMware products: • VMware Access 20.01 and 20.10 on Linux • VMware Access Connector 20.01.0.0 and 20.10 on Windows • VMware vIDM 3.3.1, 3.3.2 and 3.3.3 on Linux • VMware vIDM Connector 3.3.1, 3.3.2, 3.3.3 and 19.03 on Windows • VMware vIDM Connector 3.3.1 and 3.3.2 on Linux
Impact	Access to protected data and abuse of federated authentication.
Recommendations	NCSC-IE recommends that affected organisations should apply the appropriate updates or workarounds as recommended by WMware as soon as possible. VMware customers can access patches here. The use of strong passwords and removing access to the management interface from the internet will reduce an organisations risk.

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
certreport@decc.gov.ie
www.ncsc.gov.ie