National Cyber Security Centre

2205201000-NCSC

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

NCSC Alert

Actively Exploited Critical Vulnerabilities in VMware Products

2022-05-20

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

The NCSC is releasing this advisory to warn organisations about **critical** vulnerabilities released on 6th April and 18th May 2022 that exist in VMware products, some of which are being actively exploited.

CVE-2022-22954 (CVSSv3 9.8): VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution. Please see the VMware Advisory for more information

CVE-2022-22960 (CVSSv3 7.8): VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts. A malicious actor with local access can escalate privileges to 'root'. Please see the VMware Advisory for more information

CVE-2022-22973 (CVSSv3 7.8): VMware Workspace ONE Access and Identity Manager contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. Please see the VMware Advisory for more information

CVE-2022-22972 (CVSSv3 9.8): VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. Please see the VMware Advisory for more information.

Exploitation and chaining of CVE-2022-22954 and CVE-2022-22960 has been observed around the 12th April 2022. Reliable intelligence indicate that an unauthenticated actor with network access to the web interface leveraged CVE-2022-22954 to execute an arbitrary shell command as a VMware user. The actor then exploited CVE-2022-22960 to escalate the user's privileges to 'root'. With root access, the actor could wipe logs, escalate permissions, and move laterally to other systems. Post-exploitation, threat actors have been observed dropping webshells such as Dingo J-spy, Godzilla and tomcatjsp.

The NCSC expects that threat actors will develop exploits for the recent vulnerabilities (**CVE-2022-22973 CVE-2022-22972**) in the same VMware products in the short term.

Products Affected

- VMware Workspace ONE Access
- VMware Identity Manager (vIDM)
- VMware vRealize Automation (vRA)
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager

Impact

Remote Code Execution (RCE), Privilege Escalation, Authentication by-pass

Recommendations

The NCSC recommends strongly that organisations deploy updates per VMware Security Advisory - VMSA-2022-0014. Given the severity of these vulnerabilities, organisations should prioritise deploying this update as soon as possible.

If any of the services are exposed to the internet assume compromise and perform incident response procedures in line with your organisations Incident Response plan as a matter of urgency.

VMware have also issued workarounds for these vulnerabilities. These workarounds are meant to be a temporary solution only and will result in the loss of certain functionality, such as the ability to login for non-directory (local) users and if VMware Identity Manager is managed by vRealize Suite Lifecycle Manager, Day-2 actions like inventory sync may fail after a workaround is applied. More details on workarounds can be found at the following link: https://kb.vmware.com/s/article/88433.

If organisations Identity compromised systems they should:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organisation to provide subject matter expertise, ensure the threat actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report the details to the National Cyber Security Centre at info@ncsc.gov.ie

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