National Cyber Security Centre

0123456789-NCSC

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

# NCSC Alert

## ESXi servers worldwide encrypted using CVE-2021-21974

Tuesday 7th February, 2023

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared 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

Attackers are exploiting ESXi servers worldwide to deploy ransomware. It appears that CVE-2021-21974 is used to gain initial access to ESXi hypervisors, which provides them the ability to remotely execute code on the exploited system.

Encryption of data has been observed to be incomplete in some cases and recovery may be possible from backups – please consult the references below and contact the NCSC if affected.

Internet-exposed ESXi instances should be examined for indicators of compromise, even if there is no sign of encryption, as threat actors may have gained access and placed persistence mechanisms.

## Products Affected

The following versions of VMware ESXi are vulnerable to CVE-2021-21974:

- ESXi versions 7.x prior to ESXi70U1c-17325551
- ESXi versions 6.7.x prior to ESXi670-202102401-SG
- ESXi versions 6.5.x prior to ESXi650-202102101-SG

## Impact

Exploitation of CVE-2021-21974 could allow an attacker to remotely execute code and carry out data theft, operational disruption, ransomware and denial of service.

## Recommendations

The NCSC strongly advises system administrators to take the following actions:

- Immediately deactivate the SLP service on all ESXi hypervisors which have not yet been updated.
- NOTE: This will prevent CIM client from localising CIM servers using the SLP service. This service can be reenabled after updating the ESXi hypervisors to a non-vulnerable version.
- Apply updates to all vulnerable ESXi hypervisors where possible.

## References


- NVD: https://nvd.nist.gov/vuln/detail/CVE-2021-21974
- MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21974
- OVHcloud: https://blog.ovhcloud.com/ransomware-targeting-vmware-esxi/
- VMware: https://kb.vmware.com/s/article/76372
- Bleepingcomputer: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

**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
**LinkedIn:** ncsc-ie