UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0274

ESXIARGS RANSOMWARE TARGETS VMWARE SERVERS

DATE ISSUED: 7th February 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Unpatched and unprotected VMware ESXi servers are being targeted in a large-scale ransomware attack exploiting a vulnerability from 2021. The attack uses a new strain of ransomware named ESXiArgs, which can encrypt servers and demand a ransom payment in return for the decryption key.

BREAKDOWN

According to the French Computer Emergency Response Team (CERT-FR), attackers are actively targeting VMware ESXi servers which are unpatched against a two-year-old Remote Code Execution (RCE) vulnerability to deploy a new ESXiArgs Ransomware. The ransomware exploits the vulnerability to gain access to the server and encrypts the Virtual Machines (VMs) hosted on them. The vulnerability is tracked as CVE-2021-21974 and is caused by a stack overflow issue in the OpenSLP service. The ransomware encrypts the files on the compromised machines with the. vmxf, .vmx, .vmdk, .vmsd, and .nvram extensions and creates a .args file for each encrypted document. A ransom note named "ransom.html" and "How to Restore Your Files.html" is also released which replaces VMware ESXi's home page. The affected ESXi hypervisors are 6.x and prior to 6.7. Users with VMware Private Cloud are not affected as the SSL gateway, by design, blocks external access to the OpenSLP port (427) and protects against this type of attack.

REMEDIATION STEPS

- Update the VMware ESXi servers with the latest security patch.
- Administrators can disable the vulnerable Service Location Protocol (SLP) service on ESXi hypervisors which cannot instantly patched. See resource below.
- Monitor network activity for any suspicious or anomalous behaviour.
- Only activate necessary services and use ACL to filter access to trusted IP addresses only.
- Check out our Ransomware Defence Strategy Guide for more tips on how to secure your environment.

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

VMware https://kb.vmware.com/s/article/76372