Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Massive ESXiArgs Ransomware Attack Targets VMware ESXi Servers Worldwide

Updated: 9 February 2023

The Cybersecurity and Infrastructure Security Agency (CISA) of the United States has released a recovery script for organizations that have fallen victim to ESXiArgs ransomware. The ESXiArgs ransomware encrypts configuration files on vulnerable ESXi servers, potentially rendering virtual machines (VMs) unusable.

Organisations impacted by ESXiArgs are recommended to evaluate the script and guidance provided in the accompanying README file to determine if it is fit for attempting to recover access to files in their environment.

Organizations can access the recovery script here: https://github.com/cisagov/ESXiArgs-Recover

----

Date of Issue: 06 February 2023

Severity Level: High

Description:

Cybersecurity researchers have identified a new ransomware campaign actively targeting VMware ESXi Servers around the world. Approximately 3200 servers VMware ESXi servers worldwide have been compromised in this ransomware campaign. The ransomware dubbed as “ESXiArgs” is being deployed by exploiting a two-year-old remote code execution vulnerability. Tracked as CVE-2021-21974, the vulnerability is caused by a heap overflow issue in the OpenSLP service and this is being exploited by unauthenticated threat actors in low-complexity attacks. A patch for this vulnerability existed since 23 February 2021. Since many servers were not upgraded, they were vulnerable and could easily be exploited by the ransomware.

CERT-MU advises users to watch out for the vulnerability and apply workarounds accordingly.

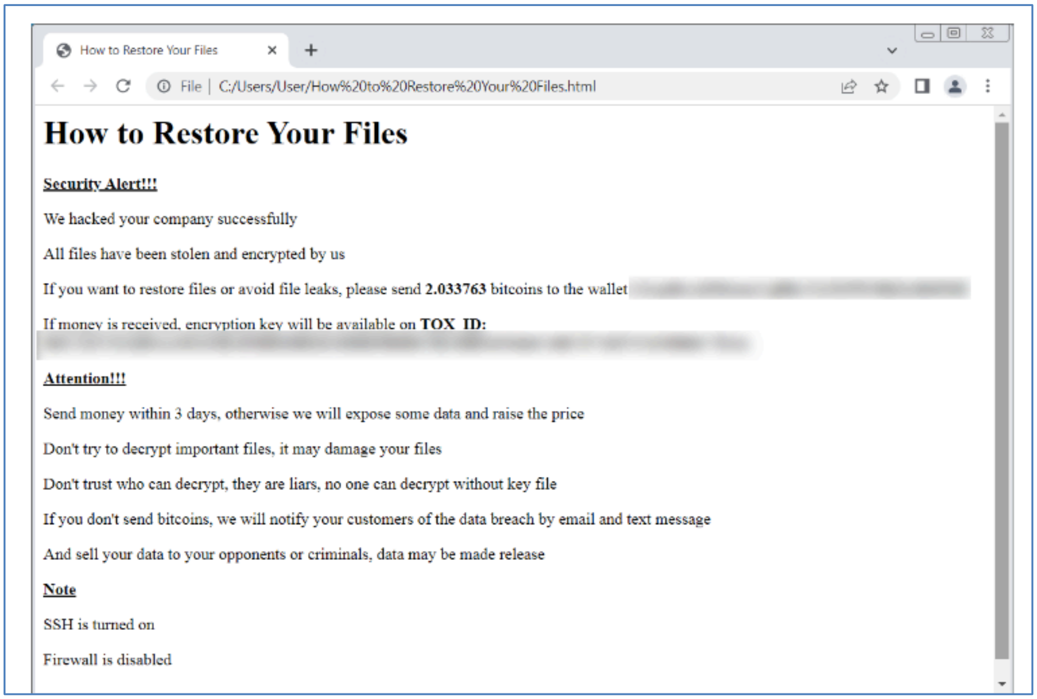
Systems Affected:

- 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

Technical Information

The ransomware encrypts files with the *.vmxf, .vmx, .vmdk, .vmsd*, and *.nvram* extensions on compromised ESXi servers and creates a *.args* file for each encrypted document with metadata.

Victims have also found ransom notes named *"ransom.html"* and *"How to Restore Your Files.html"* on locked systems.


How to Restore Your Files
File | C:/Users/User/How%20to%20Restore%20Your%20Files.html

How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.033763** bitcoins to the wallet [redacted]

If money is received, encryption key will be available on **TOX_ID:** [redacted]

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

Firewall is disabled

Workarounds

The following workarounds are recommended:

- To block incoming attacks, admins are advised to disable the vulnerable Service Location Protocol (SLP) service on ESXi hypervisors that have not yet been updated.

- It is also advised to upgrade to the latest version for VMware ESXi servers. More information about the update is available on:

https://kb.vmware.com/s/article/1014165

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org