JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

Product ID: AA23-039A
February 8, 2023

ESXiArgs Ransomware Virtual Machine Recovery Guidance

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) in response to the ongoing ransomware campaign, known as “ESXiArgs.” Malicious actors may be exploiting known vulnerabilities in VMware ESXi servers that are likely running unpatched and out-of-service or out-of-date versions of VMware ESXi software to gain access and deploy ransomware. The ESXiArgs ransomware encrypts configuration files on ESXi servers, potentially rendering virtual machines (VMs) unusable.

CISA has released an ESXiArgs recovery script at github.com/cisagov/ESXiArgs-Recover. Organizations that have fallen victim to ESXiArgs ransomware can use this script to attempt to recover their files. This CSA provides guidance on how to use the script.

ESXiArgs actors have compromised over 3,800 servers globally. CISA and FBI encourage all organizations managing VMware ESXi servers to:

- **Update servers to the latest version of VMware ESXi software**,
- **Harden ESXi hypervisors by disabling the Service Location Protocol (SLP) service,** and
- **Ensure the ESXi hypervisor is not exposed to the public internet**.

If malicious actors have compromised your organization with ESXiArgs ransomware, CISA and FBI recommend following the script and guidance provided in this CSA to attempt to recover access to your files.

Note: CISA and FBI will update this CSA as more information becomes available.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA’s 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

TECHNICAL DETAILS

Open-source reporting indicates that malicious actors are exploiting known vulnerabilities in VMware ESXi software to gain access to servers and deploy ESXiArgs ransomware. The actors are likely targeting end-of-life ESXi servers or ESXi servers that do not have the available ESXi software patches applied.[1]

ESXiArgs ransomware encrypts certain configuration files on ESXi servers, potentially rendering VMs unusable. Specifically, the ransomware encrypts configuration files associated with the VMs; it does not encrypt flat files. As a result, it is possible, in some cases, for victims to reconstruct the encrypted configuration files based on the unencrypted flat file. The recovery script documented below automates the process of recreating configuration files. The full list of file extensions encrypted by the malware is: `vmdk`, `vmx`, `vmxf`, `vmsd`, `vmsn`, `vswp`, `vmss`, `nvram`, `vmem`.

RECOVERY GUIDANCE

CISA and FBI do not encourage paying the ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, CISA and FBI urge you to promptly report ransomware incidents to a local FBI Field Office, or to CISA at cisa.gov/report.

CISA is providing these steps to enable organizations to attempt recovery of their VMs. CISA's GitHub ESXiArgs recovery script, which also outlines these steps, is available at github.com/cisagov/ESXiArgs-Recover. CISA is aware that some organizations have reported success in recovering files without paying ransoms. CISA's script is based on findings published by third-party researchers.[2]

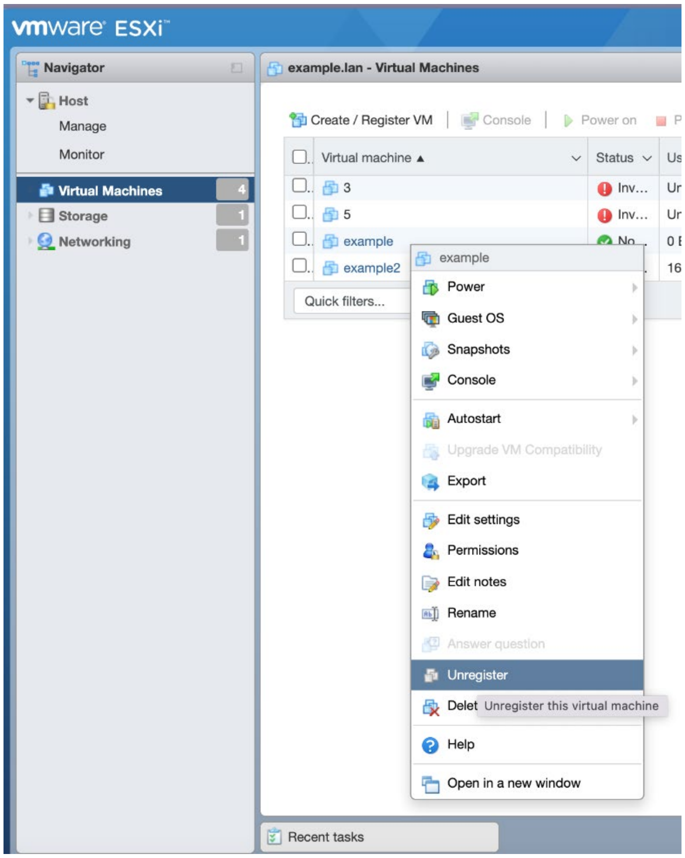
Any organization seeking to use CISA's ESXiArgs recovery script should carefully review the script to determine if it is appropriate for their environment before deploying it. This script does not seek to delete the encrypted configuration files, but instead seeks to create new configuration files that enable access to the VMs. While CISA works to ensure that scripts like this one are safe and effective, this script is delivered without warranty, either implicit or explicit. Do not use this script without understanding how it may affect your system. CISA does not assume liability for damage caused by this script. **Note:** Organizations that run into problems with the script can create a GitHub issue at https://github.com/cisagov/ESXiArgs-Recover/issues; CISA will do our best to resolve concerns.

1. **Quarantine or take affected hosts offline** to ensure that repeat infection does not occur.
2. **Download CISA's recovery script** and save it as `/tmp/recover.sh`.
    - For example, with `wget`: `wget -O /tmp/recover.sh https://raw.githubusercontent.com/cisagov/ESXiArgs-Recover/main/recover.sh`.
3. **Give the script execute permissions**: `chmod +x /tmp/recover.sh`.

4. **Navigate to the folder of a VM you would like to recover and run `ls` to view the files**.

    - **Note:** You may browse these folders by running `ls /vmfs/volumes/datastore1`. For instance, if the folder is called `example`, run `cd /vmfs/volumes/datastore1/example`.

5. **View files by running `ls`. Note the name of the VM** (via naming convention: `[name].vmdk`).
6. **Run the recovery script** with `/tmp/recover.sh [name]`, where `[name]` is the name of the VM determined previously.
    a. If the VM is a thin format, run `/tmp/recover.sh [name] thin`.
    b. If successful, the recovery script will output that it has successfully run. If unsuccessful, it may not be possible for the recovery script to recover your VMs; consider engaging external incident response help.
7. If the script succeeded, **re-register the VM**.
    a. If the ESXi web interface is inaccessible, **remove the ransom note and restore access** via the following steps. (**Note:** Taking the steps below moves the ransom note to the file `ransom.html`. Consider archiving this file for future incident review.)
        i. Run `cd /usr/lib/vmware/hostd/docroot/ui/ && mv index.html ransom.html && mv index1.html index.html`.
        ii. Run `cd /usr/lib/vmware/hostd/docroot && mv index.html ransom.html && rm index.html && mv index1.html index.html`.
        iii. **Reboot the ESXi server** (e.g., with the `reboot` command). After a few minutes, you should be able to navigate to the web interface.
    b. In the ESXi web interface, **navigate to the Virtual Machines page**.
        i. If the VM you restored already exists, right click on the VM and select `Unregister` (see figure 1).

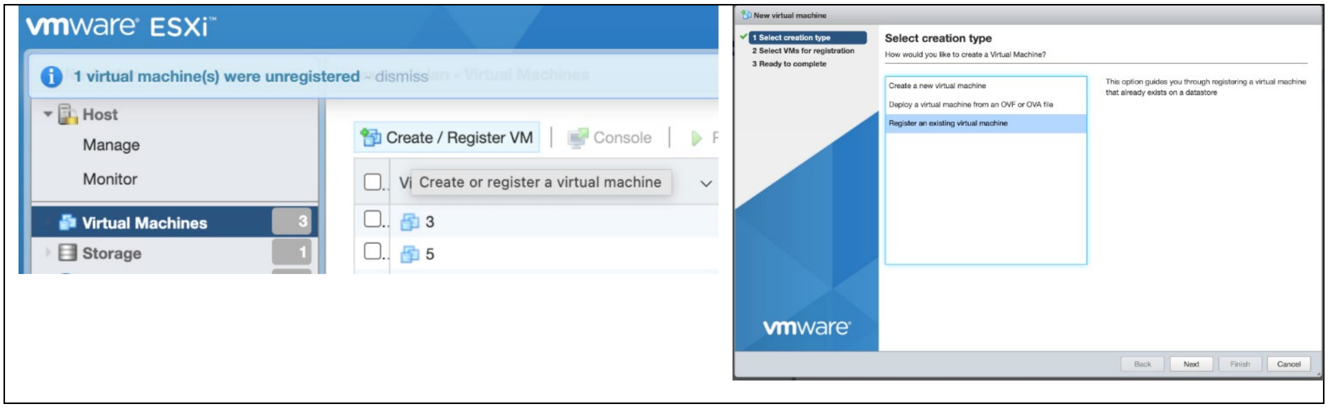


Unregister this virtual machine

Figure 1: Unregistering the virtual machine

ii. Select `Create / Register VM` (see figure 2).

iii. Select `Register an existing virtual machine` (see figure 2).



1 virtual machine(s) were unregistered - dismiss

Create or register a virtual machine

Select creation type

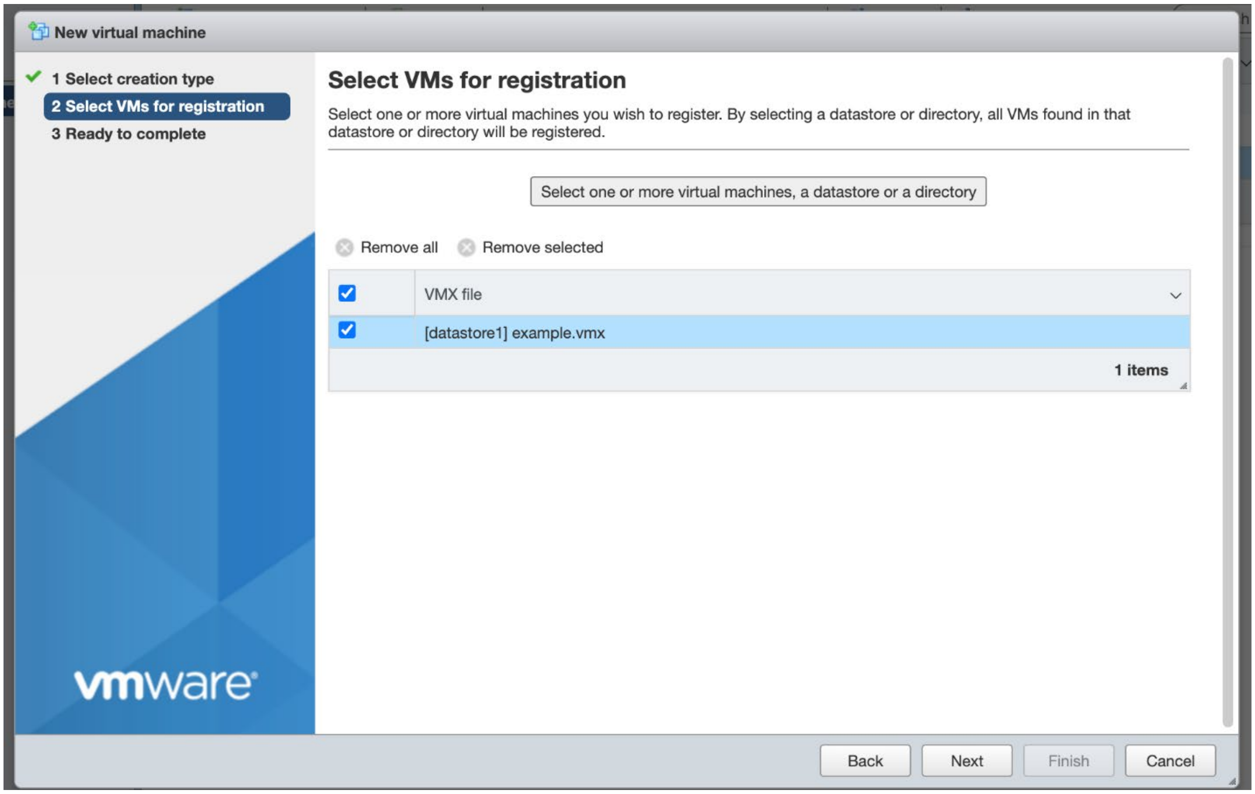
How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through registering a virtual machine that already exists on a datastore

Figure 2: Registering the virtual machine, selecting machine to register

iv. Click `Select one or more virtual machines, a datastore or a directory` to navigate to the folder of the VM you restored. Select the `vmx` file in the folder (see figure 3).



Select VMs for registration

Select one or more virtual machines you wish to register. By selecting a datastore or directory, all VMs found in that datastore or directory will be registered.

☑ [datastore1] example.vmx

Figure 3: Registering the virtual machine, finalizing registration

v. Select `Next` and `Finish`. You should now be able to use the VM as normal.

8. **Update servers to the latest software version, disable the Service Location Protocol (SLP) service, and ensure the ESXi hypervisor is not configured to be exposed to the public internet** before putting systems back online.

Additional Incident Response

The above script only serves as a method to recover essential services. Although CISA and FBI have not seen any evidence that the actors have established persistence, we recommend organizations take the following additional incident response actions after applying the script:

1. Review network logging to and from ESXi hosts and the guest VMs for unusual scanning activity.
2. Review traffic from network segments occupied by the ESXi hosts and guests. Consider restricting non-essential traffic to and from these segments.

If you detect activity from the above, implement your incident response plan. CISA and FBI urge you to promptly report ransomware incidents to a local FBI Field Office, or to CISA at cisa.gov/report. Organizations should also collect and review artifacts, such as running processes/services, unusual authentications, and recent network connections.

See the joint CSA from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious

Activity for additional guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA also encourages government network administrators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail steps for both incident and vulnerability response.

Additional resources for recovering `.vmdk` files can be found on a third-party researcher's website.[2]

MITIGATIONS

Note: These mitigations align with the cross-sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs, including additional recommended baseline protections, see cisa.gov/cpg.

CISA and FBI recommend all organizations:

- Temporarily remove connectivity for the associated ESXi server(s).
  - **Upgrade your ESXi servers to the latest version of VMware ESXi software** [CPG 5.1]. ESXi releases are cumulative, and the latest builds are documented in VMware's article, Build numbers and versions of VMware ESXi/ESX.
  - **Harden ESXi hypervisors by disabling the Service Location Protocol (SLP) service,** which ESXiArgs may leverage. For more information on executing workarounds, see VMware's guidance How to Disable/Enable the SLP Service on VMware ESXi.
  - **Ensure your ESXi hypervisor is not configured to be exposed to the public internet.**

In addition, CISA and FBI recommend organizations apply the following recommendations to prepare for, mitigate/prevent, and respond to ransomware incidents.

Preparing for Ransomware

- Maintain offline backups of data, and regularly test backup and restoration [CPG 7.3]. These practices safeguard an organization's continuity of operations or at least minimize potential downtime from a ransomware incident and protect against data losses.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response procedures for a ransomware incident [CPG 7.1, 7.2].

Mitigating and Preventing Ransomware

- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
- Require phishing-resistant MFA for as many services as possible [CPG 1.3]—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement allow-listing policies for applications and remote access that only allow systems to execute known and permitted programs.
- Open document readers in protected viewing modes to help prevent active content from running.
- Implement user training program and phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- Use strong passwords [CPG 1.4] and avoid reusing passwords for multiple accounts. See CISA Tip Choosing and Protecting Passwords and the NIST's Special Publication 800-63B: Digital Identity Guidelines for more information.
- Require administrator credentials to install software [CPG 1.5].
- Audit user accounts with administrative or elevated privileges and configure access controls with least privilege in mind [CPG 1.5].
- Install and regularly update antivirus and antimalware software on all hosts.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- **Consider participating in CISA's no-cost Automated Indicator Sharing (AIS)** program to receive real-time exchange of machine-readable cyber threat indicators and defensive measures.

Responding to Ransomware Incidents

If a ransomware incident occurs at your organization:

- Follow your organization's Ransomware Response Checklist (see Preparing for Ransomware section).
- Scan backups. If possible, scan backup data with an antivirus program to check that it is free of malware. This should be performed using an isolated, trusted system to avoid exposing backups to potential compromise.
- Follow the notification requirements as outlined in your cyber incident response plan.

- Report incidents to CISA at cisa.gov/report, FBI at a local FBI Field Office, or the U.S. Secret Service (USSS) at a USSS Field Office.
- Apply incident response best practices found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: CISA and FBI strongly discourage paying ransoms as doing so does not guarantee files and records will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.

RESOURCES

See Stopransomware.gov, a whole-of-government approach, for ransomware resources and alerts.

REFERENCES

[1] VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks - VMware Security Blog

[2] Enes Sonmez and Ahmet Aykac, YoreGroup Tech Team: decrypt your crypted files in ESXi servers affected by CVE-2020-3992 / CryptoLocker attack

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA and FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or FBI.

ACKNOWLEDGEMENTS

CISA and FBI would like to thank VMware for their contributions to this CSA.