ESXiArgs: Questions & Answers

VMware Security

© VMware LLC.

Table of contents

ESXiArgs: Questions & Answers

Introduction

The “ESXiArgs” ransomware attacks appear to be targeting unpatched and unprotected instances of VMware ESXi. The VMware Security Response Center has issued a statement about these issues:

VMware Security Response Center (vSRC) Response to ‘ESXiArgs’ Ransomware Attacks

as well as additional clarification about the substantial security and lifecycle (update & upgrade) automation capabilities found in VMware vSphere:

vSphere Security: Proactive and Continuous

This document is meant to address other questions and provide additional resources.

Current Update

Updated at 0900 PST on February 16, 2023.

Next Expected Update

There is not a regular update schedule for this document.

Links

- VMware Security Response Center (vSRC) Response to ‘ESXiArgs’ Ransomware Attacks (VMware’s response to this issue)
- vSphere Security: Proactive and Continuous (blog post highlighting the security capabilities of vSphere, protecting both itself and workloads)
- CISA ESXiArgs Ransomware Recovery script (a script that CISA developed to rebuild VMDK file metadata – not supported by VMware, see below)
- vSphere Security Configuration Guides (baseline hardening guidance for VMware vSphere)
- Tips for Patching VMware vSphere (practical advice for ensuring patching success, and many ideas here apply to other components as well)
- VMware Ransomware Resource Center (guidance on tactics to help prevent, deter, and recover from attacks)
- VMware Security Advisories (list of all disclosed security vulnerabilities)
- VMware Security Advisory Mailing List (please subscribe for proactive notifications of security advisories)

Q&A

Who is affected by this?

The primary impact is to organizations that are running unpatched versions of ESXi, where attackers also have direct access to ESXi management interfaces.

When do people need to act?

Organizations that are running versions of software older than current releases are at risk and should be updated to the latest versions immediately. Customer security personnel should make assessments of more nuanced situations; for assistance with security assessments please engage VMware Professional Services.

Organizations that place their IT infrastructure systems' management interfaces directly on the Internet should take immediate steps to verify filters and additional security controls in front of them, reviewing those controls for effectiveness.

Is this issue being exploited "in the wild?"

Yes.

What CVEs are involved in these attacks?

Unknown currently. The media has speculated about the involvement of CVE-2022-31699, CVE-2021-21995, CVE-2021-21974, CVE-2020-3992, and CVE-2019-5544 but it is very likely that the attackers are using any vulnerability that is accessible to them. VMware is continuing to investigate.

Is this a vulnerability in VMware products?

VMware believes that these attacks leverage existing vulnerabilities in VMware products, that already have been resolved through updates. This does not appear to be a new vulnerability. However, we continue to monitor the situation as it evolves.

What products are affected?

VMware ESXi.

What patch level do I need to be at to avoid this issue?

The latest patches to all major supported VMware product versions resolve all disclosed vulnerabilities. Any software, from VMware or others, which is down-level from the current released version may present a security risk. Bring environments up to the latest supported releases.

Does ESXi build resolve this issue?

A particular release of a product may resolve specific issues, but still contain other vulnerabilities. Bring environments up to the latest supported releases to resolve all disclosed vulnerabilities.

Will there be a patch to vSphere 6.0, 6.5, and 6.7 to resolve this issue?

vSphere 6.x versions are beyond their supported lifespan and are no longer being updated. Additionally, ransomware is not something you directly patch. Malware of this type is usually a toolkit that exploits other vulnerabilities. The vulnerabilities that appear to be used by ESXiArgs already have patches.

Is there a workaround available for this issue?

VMware's general recommendations for customers who wish to improve security are:

- Run supported versions of VMware software.
- Stay updated to the latest releases of VMware software, in a prompt fashion.
- Use the vSphere Security Configuration Guides to harden environments.
- Tightly control access to IT infrastructure management interfaces (not just vSphere).
- Use multifactor authentication and good authorization practices.
- Subscribe to the VMware Security Advisory mailing lists for proactive notification of issues.

Organizations that place their IT infrastructure systems' management interfaces directly on the Internet should take immediate steps to verify filters and additional security controls in front of them, reviewing those controls for effectiveness.

Security is very dependent on context, and VMware cannot provide advice without knowing more about a customer's environment and business. For this level of assistance please engage VMware Professional Services.

Why isn't VMware releasing a security advisory about this?

This attack does not exploit a new vulnerability, so there is no cause to issue a product advisory.

Is VMware making a statement about this ransomware?

VMware has published a response that will be updated as needed:

VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks

What can I do to protect my environment from this type of malware?

VMware's general recommendations for customers who wish to improve security are:

- Run supported versions of VMware software.
- Stay updated to the latest releases of VMware software, in a prompt fashion.
- Use the vSphere Security Configuration Guides to harden environments.
- Tightly control access to IT infrastructure management interfaces (not just vSphere).
- Use multifactor authentication and good authorization practices.
- Subscribe to the VMware Security Advisory mailing lists for proactive notification of issues.

Organizations that place their IT infrastructure systems' management interfaces directly on the Internet should take immediate steps to verify filters and additional security controls in front of them, reviewing those controls for effectiveness.

Security is very dependent on context, and VMware cannot provide advice without knowing more about a customer's environment and business. For this level of assistance please engage VMware Professional Services.

Are there tools available to help recover from the ESXiArgs attack?

CISA 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 making virtual machines (VMs) unusable. This tool was developed in conjunction with VMware but isn't supported directly by VMware. Should customers run into any problems with the tool, they can create a GitHub issue here: https://github.com/cisagov/ESXiArgs-Recover/issues and CISA will do their best to resolve concerns. For more information: https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script

VMware cannot give advice about the effectiveness of third-party tools. As with all breaches, please consult your incident response team prior to executing recovery steps.

There are blog posts on the Internet saying that if I make specific changes I can stop ESXi ransomware. Do those work?

To understand how to stop ransomware you need to first understand what it is and is not. Ransomware is not a single vulnerability or type of attack. It is not something that can be patched directly, though patching systems does remove vulnerabilities that attackers can use to break in.

What ransomware is, though, is the end stage of a breach that may also involve exfiltration of data, extortion of the primary victim, and extortion of the victim's customers. These breaches are executed over months or years, by humans who customize attacks for different victims. The only single approach to stop ransomware that is effective is shutting the machine off completely (but obviously undesired – availability is a key part of security, too).

Organizations with effective defenses against ransomware use a multi-layered approach, implementing defense-in-depth with technology and process changes. These include patching, perimeter security controls, multifactor authentication, and more. Many of these tactics are discussed in papers in the Ransomware Resource Center. One single change to a security control does not stop attacks.

Security is always a tradeoff, and often that tradeoff is with system usability and performance. System hardening guidance from VMware, such as the Security Configuration Guides, must balance product functionality with security, and must ensure that the product continues to work as expected or that changes to functionality are well documented so that virtualization administrators can make a good decision in the context of their own environments.

Guidance found on the internet is not bound by these same constraints. Caution should always be used with any information on the internet to ensure that it does not misrepresent the effectiveness of the approach, and that it accurately portrays the tradeoffs and negative effects that may be experienced from implementing it. When in doubt, please engage appropriate legal, business, technical, and audit expertise for a review.

Additionally, "security through obscurity" is the information security phrase for attempting to hide things so that attackers will not find them. Examples of this include not using reverse DNS (PTR) records, renaming administrator and root accounts, and more. Security through obscurity is not considered a valid security posture, though it can lead to attackers generating log entries that can be monitored for as signs of intrusion. These types of tactics cause additional work for IT staff, increase the likelihood of human error, may break connectivity between systems, and create support issues and risks. These tactics may also create additional attack surface, usually unintentionally, which is counterproductive.

Discuss the effectiveness of any of these types of controls with your security team and risk management staff prior to implementing them.

Is there a way to automate auditing and deactivating SLP services on all my ESXi hosts?

Yes. Please see the vSphere Security Configuration Guide for an example in PowerCLI. Remember that unpatched SLP may not be the only attack vector in use, and other types of attacks may exploit other vulnerabilities.

If I disable SLP will CIM functionality be affected?

Yes. Alternately you can patch ESXi so that SLP no longer contains vulnerabilities and is safe to use.

What functionality do I lose if SLP (and CIM) are disabled?

You may lose third-party monitoring and management functionality if you are using those protocols. No vSphere or VMware product interoperability is affected.

Use of CIM and SLP are not common. Every environment is different, but you may be able to test the effect of this change by altering a single ESXi host first, observing the effect, then altering the rest of the hosts to match.

If I disable SLP am I safe?

Attackers do not share their plans with their victims proactively, so there is no guarantee that the SLP vulnerabilities are the only ones in use. Please update to the latest versions of the products to remove ALL disclosed vulnerabilities.

Additionally, security is very dependent on context. VMware cannot generally make statements about being “safe” – for a comprehensive review of your security controls and their effectiveness please engage VMware Professional Services.

Is VMware Cloud on AWS affected?

No. VMware Cloud on AWS is managed and updated by teams of administrators who resolved vulnerabilities as needed. The vulnerabilities implicated in these attacks were resolved years ago.

Is VMware Cloud Foundation affected?

Customers should ensure that they have updated their VMware Cloud Foundation installations to the latest supported versions of software.

Can I just firewall the affected products?

Firewalling and other forms of network isolation can be a compensating control, helping to mitigate the issue. All organizations have different environments and needs. Whether firewalls are appropriate compensating controls in your environment for this situation is for you and your information security staff to assess.

Is vSphere 5.5 affected?

Most likely. vSphere 5.5 is past the end of general and extended support and is not evaluated as part of security advisory and response work. Please upgrade to vSphere 7 or newer as soon as possible. There is a terrific upgrade starting point at https://core.vmware.com/guide-vsphere-70-upgrade!

Is vSphere 6.0 affected?

Yes. vSphere 6.0 is past the end of general and extended support and is not evaluated as part of security advisory and response work. Please upgrade to vSphere 7 or newer as soon as possible. There is a terrific upgrade starting point at https://core.vmware.com/guide-vsphere-70-upgrade!

Is vSphere 6.5 affected?

Some versions of vSphere 6.5 contained the vulnerabilities that are currently associated with these attacks. Please update to the latest versions of 6.5 and make plans to upgrade to vSphere 7 or newer as soon as possible. There is a terrific upgrade starting point at https://core.vmware.com/guide-vsphere-70-upgrade!

Is vSphere 6.7 affected?

Some versions of vSphere 6.7 contained the vulnerabilities that are currently associated with these attacks. Please update to the latest versions of 6.7 and make plans to upgrade to vSphere 7 or newer as soon as possible. There is a terrific upgrade starting point at https://core.vmware.com/guide-vsphere-70-upgrade!

Is vSphere 7.0 affected?

Some versions of vSphere 7.0 contained the vulnerabilities that are currently associated with these attacks. Please update to the latest patch levels of vSphere 7 Update 3.

Is vSphere 8.0 affected?

No.

Is CVE-2021-21974 tied to the latest ransomware attacks?

This has been reported by multiple publications. VMware currently has no evidence to support that a new vulnerability is being used to propagate recent ransomware attacks, but there is also no evidence that CVE-2021-21974 is the only attack vector, either. VMware's recommendation is to ensure customers patch to the latest version.

I have verified OpenSLP is enabled on my ESXi hosts. What actions should I take?

VMware has recommended disabling the OpenSLP service on ESXi since 2021. The steps to disable OpenSLP are in KB 76372 or listed in the Security Configuration Guide.

Changelog

All times are in Pacific Standard (-0800)

2023-02-06, 1200: Initial release.

2023-02-07, 0700: Minor updates for clarity.

2023-02-08, 0600: Updates for clarity, addition of links for the CISA.gov recovery script.

2023-02-09, 0700: Updates to clarify attack vectors.

2023-02-13, 0900: Updates for clarity, updated link for resources.

2023-02-16: 0900: Added “If I disable SLP am I safe?” and revised the answer to “If I disable SLP will CIM functionality be affected?” and added a link to the vSphere blog.

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

© VMware LLC.

© VMware LLC.

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.