ESXiArgs Ransomware Targets Publicly-Exposed ESXi OpenSLP Servers | Recorded Future

By German Hoeffner, Aaron Soehnen & Gianni Perez

Archived: 2026-04-05 23:51:18 UTC

An ongoing ransomware campaign dubbed ESXiArgs is targeting outdated VMware ESXi installations. While first reports surfaced on Friday, February 3rd, a more significant wave infected at least 2,000 hosts over the weekend, according to BleepingComputer. An internet-wide scan reported up to 8,000 infected hosts as of this writing.

The attack likely exploits CVE-2021-21974, a two-year-old remote code execution vulnerability in the bundled OpenSLP service, for which a patch has been available since February 2021.

VMware ESXi is a Type 1 hypervisor that runs directly on host server hardware, providing a virtualization layer capable of abstracting CPU, storage, memory, and networking resources into multiple virtual machines. OpenSLP is an open-source framework for networking applications to discover the existence, location, and configuration of services in enterprise networks, which ESXi client applications use to resolve network addresses and hosts.

Affected Systems

The following ESXi versions are affected by CVE-2021–21974:

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

For a system to be vulnerable to CVE-2021–21974, the OpenSLP service needs to be running, and its associated port 427 needs to be reachable from the internet. According to VMware, this service is disabled by default on new installations since ESXi 7.0 U2c and ESXi 8.0 GA.

It should be noted that CVE-2021-21974 is not yet officially confirmed as the attack vector. The French CERT lists CVE-2020-3992 as another possibility, which is also a vulnerability of OpenSLP. While the exact vulnerability is unknown, OVHcloud, a large hoster with ESXi servers in its portfolio, confirmed that the OpenSLP service is the point of entry used in this campaign. VMware also recommends disabling OpenSLP as mitigation.

Furthermore, OVHcloud blocked port 427 for all servers with ESXi installed. Besides being assigned to the OpenSLP service, this port may also be used by a backdoor script in compromised installations.

Mitigation and recovery

VMware recommends updating vulnerable ESXi servers to an unaffected version if possible. As an additional measure, the OpenSLP service can be disabled. The procedure for this is described in this document.

Current insights by OVH and the security community suggest that closing port 427 or restricting access to it might also mitigate this vulnerability as a stop-gap measure.

Infected systems will have the following files present in the /tmp folder, which can serve as an indicator of compromise:

- encrypt
- encrypt .sh
- public.pem

The system's motd (message of the day) file and index.html will be replaced with a ransom note after the encryption process. The ransomware will try to stop running VMs to be able to encrypt their associated files.

The encryption algorithm has no known weaknesses that allow decrypting files without the key. But according to OVHcloud, stopping the VMs often fails, which leaves the files locked and prevents any encryption. Even if the encryption succeeds, only small chunks of the files are encrypted, which makes a recovery theoretically possible. However, this process is quite difficult, and security analysts are still working on the best procedures. The current procedure is described in this blog post.

Additionally, CISA and the FBI have released an ESXiArgs Ransomware Recovery Guidance, including a specific recovery script for this type of ransomware attack. We encourage all affected organizations to follow this recovery guidance.

Summary

VMware identified a new ransomware campaign targeting public-facing ESXi servers worldwide. The attackers are likely leveraging a two-year-old heap overflow vulnerability in ESXi's OpenSLP service. Patches for this vulnerability have been available, but the attack has revealed that many servers may still be vulnerable. Users should upgrade to the latest ESXi version and restrict access to the OpenSLP service to trusted IP addresses to mitigate potential threats if patching isn't readily available.

This content was originally published February 8, 2023 and updated February 9, 2023.
