SISA ProACT MDR Solution: Threat Advisory: VMware ESXi servers worldwide are being targeted by Massive ESXiArgs ransomware attack

Threat Severity: Critical
Published on: 5th Feb 2023

www.sisainfosec.com

VMware ESXi servers worldwide are being targeted by Massive ESXiArgs ransomware attack

Summary:

Unpatched VMware ESXi servers are being actively argeted by attackers to deploy a new ESXiArgs ransomware against a two-year-old remote code execution vulnerability.

Risk Scoring

CVE-ID	CVSSv3 Score
CVE-2021-21974	**8.8**

Affected Products:

ESXi versions: 6.x and prior to 6.7:

- 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

Vulnerability Details:

OpenSLP as used in ESXi has a **heap-overflow vulnerability**. A malicious actor residing within the same network segment as ESXi who has access to **port 427** may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.

Ransomware Attack Campaigns

At least 120 VMware ESXi servers worldwide have already been compromised in this ransomware campaign. The ransom notes seen in this attack appear to be from a new ransomware family.

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 (likely needed for decryption). ID Ransomware's Michael Gillespie is currently tracking the ransomware under the name '**ESXiArgs**.

The following files are stored in the /tmp folder of a breached server:

- **encrypt** - The encryptor ELF executable.

- **encrypt.sh** - A shell script that acts as the logic for the attack, performing various tasks before executing the encryptor, as described below.
- **public.pem** - A public RSA key used to encrypt the key that encrypts a file.
- **motd** - The ransom note in text form that will be copied to /etc/motd so it is shown on login. The server's original file will be copied to /etc/motd1.
- **index.html** - The ransom note in HTML form that will replace VMware ESXi's home page. The server's original file will be copied to index1.html in the same folder.

Among various other tasks carried out by the the script **encrypt.sh including encryption of the files,** it is observed to perform a some cleanup, removing a backdoor installed to **/store/packages/vmtools.py** and deleting various lines from the following files:

- /var/spool/cron/crontabs/root
- /bin/hostd-probe.sh
- /etc/vmware/rhttpproxy/endpoints.conf
- /etc/rc.local.d/local.sh

Indicators of Compromise:

Path:

- /store/packages/vmtools.py

Hash:

- 773d147a031d8ef06ee8ec20b614a4fd9733668efeb2b05aa03e36baaf082878

Recommendations:

- To block incoming attacks, admins have to disable the vulnerable Service Location Protocol (SLP) service on ESXi hypervisors that haven't yet been updated
- Apply the patch as soon as possible
- Systems left unpatched should be scanned to look for signs of compromise
- Ensure your data are backed up
- Make sure only necessary services are active and filtered with ACL to only trusted IP adresses
- Monitor your system for any abnormal behaviour.
- All admins whose servers are compromised should check for the existence of this **vmtools.py** file to make sure it was removed. If found, the file should be removed immediately

Ending Note:

Investigations are still being carried out on the ongoing ransomware attack campaigns.

Reference:

- https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- https://www.bleepingcomputer.com/news/security/google-fi-data-breach-let-hackers-carry-out-sim-swap-attacks/
- https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
- https://blog.ovhcloud.com/ransomware-targeting-vmware-esxi/
- https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/
- https://kb.vmware.com/s/article/76372