ESXiArgs Ransomware Hits Over 3,800 Servers as Hackers Continue Improving Malware

There have been some new developments in the case of the ESXiArgs ransomware attacks, including related to the encryption method used by the malware, victims, and the vulnerability exploited by the hackers.

After the US Cybersecurity and Infrastructure Security Agency (CISA) announced the availability of an open source tool designed to help some victims of the ESXiArgs ransomware recover their files without paying a ransom, the FBI and CISA released a document providing recovery guidance.

The FBI and CISA are aware of more than 3,800 servers that were compromised around the world in ESXiArgs ransomware attacks.

Currently, the Shodan and Censys search engines show 1,600-1,800 hacked servers, but there is indication that many impacted organizations have started responding to the attack and cleaning up their systems.

Reuters has conducted an analysis and determined that the victims include Florida’s Supreme Court and universities in the United States and Europe.

An analysis of the file-encrypting malware deployed in the ESXiArgs attacks showed that it has targeted files associated with virtual machines (VMs). However, experts noticed that the ransomware mainly targeted VM configuration files, but did not encrypt the flat files that store data, allowing some users to recover their data.

The tool released by the US government reconstructs the encrypted configuration files based on the unencrypted flat files.

However, Bleeping Computer reported on Wednesday that some victims have been targeted with a new version of the ESXiArgs malware, one with a different encryption process that involves encrypting more data, which prevents the recovery of files.

Until now, the ransomware did not encrypt the majority of data in large files, but the new version of the malware encrypts a

far more significant amount of data in large files. Up until now, researchers have not found any flaws in the actual encryption, making it impossible to restore encrypted files.

It has been assumed that the ESXiArgs attacks leverage CVE-2021-21974 for initial access. This is a high-severity remote code execution vulnerability in VMware ESXi that VMware patched in February 2021. The issue is related to OpenSLP.

VMware has not confirmed exploitation of CVE-2021-21974, but it did say that there is no evidence of a zero-day vulnerability being leveraged in the attacks.

However, threat intelligence company GreyNoise is not convinced that there is enough evidence that CVE-2021-21974 is being exploited. GreyNoise pointed out that several OpenSLP-related vulnerabilities have been found in ESXi in recent years, and any of them could have been exploited in the ESXiArgs attacks, including CVE-2020-3992 and CVE-2019-5544.

Data collected by cloud security company Wiz showed that, as of February 7, 12% of ESXi servers were unpatched against CVE-2021-21974 and vulnerable to attacks.

The attacks have yet to be attributed to a known threat actor, but the evidence collected so far suggests that the file-encrypting malware is based on Babuk source code that was leaked in 2021.

“Due to the relatively low ransom demand (2 BTC) and widespread, opportunistic targeting, we assess with moderate confidence this campaign is not tied to ransomware groups known for ‘Big Game Hunting’,” said SOC-as-a-service provider Arctic Wolf. “More established ransomware groups typically conduct OSINT on potential victims before conducting an intrusion and set the ransom payment based on perceived value.”

Related: VMware Patches VM Escape Flaw Exploited at Geekpwn

Event

Related: VMware Confirms Exploit Code Released for Critical vRealize Logging Vulnerabilities

> *ESXiArgs Ransomware Hits Over 3,800 Servers as Hackers Continue Improving Malware*