VMware Says No Evidence of Zero-Day Exploitation in ESXiArgs Ransomware Attacks

VMware has urged customers to take action as unpatched ESXi servers continue to be targeted in ESXiArgs ransomware attacks.

Hackers are exploiting CVE-2021-21974, a high-severity ESXi remote code execution vulnerability related to OpenSLP that VMware patched in February 2021. Following successful exploitation, unidentified threat actors have deployed file-encrypting ransomware that targets virtual machines.

Technical details and a proof-of-concept (PoC) exploit for CVE-2021-21974 have been around for nearly two years, but there is no indication that in-the-wild exploitation has been observed until now.

In a blog post published on its Security Response Center on Monday, VMware said there is no evidence that the attacks involve exploitation of a zero-day vulnerability.

“Most reports state that End of General Support (EOGS) and/or significantly out-of-date products are being targeted with known vulnerabilities which were previously addressed and disclosed in VMware Security Advisories,” the virtualization giant said.

Attacks are possible because many organizations are running old and unpatched software.

“I’ve assessed nearly 500 owned boxes this evening, all of them are on old software releases. A shocking amount of orgs run ESXi on long end of life versions,” researcher Kevin Beaumont said on Monday.

ESXiArgs ransomware attacks appear to have started on or around February 3. As of February 7, Censys shows nearly 2,500 compromised servers and Shodan shows more than 1,600. Most of the hacked systems are located in France, followed by the United States.

On compromised systems, the hackers drop a ransom note instructing victims to pay roughly $50,000 in bitcoins in order to recover their files and prevent them from getting leaked. While the cybercriminals claim to have stolen data that they will sell unless a ransom is paid, there does not appear to be any evidence to date that files have actually been stolen in ESXiArgs attacks.

As for the malware used in these attacks, it seems to target files associated with virtual machines.

In some cases, the malware’s encryption routine can partially fail, which could allow some victims to recover their data without paying a ransom. However, recovering files that have been properly encrypted seems impossible for the time being.

Cyble has published a technical analysis of the malware, including information on VM configuration file modifications, file encryption, persistence, and cleanup.

Government cybersecurity agencies around the world, including in the United States, have issued alerts over the ESXiArgs ransomware attacks.

Related: VMware Patches VM Escape Flaw Exploited at Geekpwn Event

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

VMware Says No Evidence of Zero-Day Exploitation in ESXiArgs Ransomware Attacks