VMware: Patch Horizon servers against ongoing Log4j attacks!

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** January 25, 2022 04:19 PM **0**

VMware urges customers to patch critical Log4j security vulnerabilities impacting Internet-exposed VMware Horizon servers targeted in ongoing attacks.

Following successful exploitation, threat actors deploy custom web shells (https://twitter.com/GossiTheDog/status/1484145056198053891) into the VM Blast Secure Gateway service to gain access to organizations'

networks, according to a recent NHS Digital report about VMware Horizon systems attacked with Log4Shell exploits (http://digital.nhs.uk/cyber-alerts/2022/cc-4002).

This allows them to carry out various malicious activities, including data exfiltration and deployment of additional malware payloads such as ransomware.

Microsoft also warned two weeks ago of a Chinese-speaking threat actor tracked as DEV-0401 who deploys Night Sky ransomware on Internet-exposed VMware Horizon servers (https://www.bleepingcomputer.com/news/security/night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/) using Log4Shell exploits.

In an email to Bleeping Computer today, VMware said they are strongly urging customers to patch their Horizon servers to defend against these active attacks.

"Even with VMware's Security Alerts and continued efforts to contact customers directly, we continue to see that some companies have not patched," Kerry Tuttle, VMware's Corporate Communications Manager, told BleepingComputer.

"VMware Horizon products are vulnerable to critical Apache Log4j/Log4Shell vulnerabilities unless properly patched or mitigated using the information provided in our security advisory, VMSA 2021-0028 (https://www.vmware.com/security/advisories/VMSA-2021-0028.html), which was first published on Dec. 10, 2021, and updated regularly with new information.

"Customers who have not applied either the patch or the latest workaround provided in VMware's security advisory are at risk of being compromised—or may have already been compromised—by threat actors

who are leveraging the Apache Log4shell vulnerability to actively compromise unpatched, internet-facing Horizon environments."

Admins warned not to let their guard down

VMware's call to action follows a similar warning issued last week by the Netherlands' National Cybersecurity Centre (NCSC), urging Dutch organizations to remain vigilant in the face of ongoing threats represented by Log4j attacks (https://www.bleepingcomputer.com/news/security/dutch-cybersecurity-agency-warns-of-lingering-log4j-risks/).

The Dutch government agency cautioned that malicious actors will keep searching for vulnerable servers they can breach in targeted attacks and asked orgs to applyLog4j security updates or mitigating measures where necessary.

According to Shodan (https://www.shodan.io/search?query=title%3A%22VMware+Horizon%22), there are tens of thousands of Internet-exposed VMware Horizon servers, which all need to be patched against Log4j exploitation attempts.

Log4j security flaws (including Log4Shell) are a very appealing attack vector for state-backed and financially motivated attackers since this open-source Apache logging library is used in software products from dozens of vendors (https://www.bleepingcomputer.com/news/security/log4j-list-of-vulnerable-products-and-vendor-advisories/).

The Log4Shell remote code execution vulnerability (https://www.bleepingcomputer.com/tag/log4shell/), in particular, can be exploited remotely on servers exposed to local or Internet access to enable attackers to move laterally across a network until they gain access to sensitive internal systems.

After its disclosure, multiple threat actors started using Log4Shell exploits in the wild (https://www.bleepingcomputer.com/news/security/log4j-vulnerability-

now-used-by-state-backed-hackers-access-brokers/), including state-backed hacking groups from China, Iran, North Korea, and Turkey, as well as access brokers used by ransomware gangs.

"Any time we see vulnerabilities that are as far reaching as Log4j, it is critical that all impacted users move quickly to implement security responses," Tuttle also told BleepingComputer today.

"VMware strongly recommends that customers visit VMSA-2021-0028 (https://www.vmware.com/security/advisories/VMSA-2021-0028.html) and apply the guidance for Horizon. VMware prioritizes the security of our customers as we continue to respond to the industry-wide impact of the Apache Log4j vulnerabilities."

Related Articles:

FTC warns companies to secure consumer data from Log4J attacks (https://www.bleepingcomputer.com/news/security/ftc-warns-companies-to-secure-consumer-data-from-log4j-attacks/)

US orders federal govt agencies to patch critical Log4j bug (https://www.bleepingcomputer.com/news/security/us-orders-federal-govt-agencies-to-patch-critical-log4j-bug/)

Conti ransomware uses Log4j bug to hack VMware vCenter servers (https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/)

Log4j: List of vulnerable products and vendor advisories (https://www.bleepingcomputer.com/news/security/log4j-list-of-vulnerable-products-and-vendor-advisories/)

Dutch cybersecurity agency warns of lingering Log4j risks (https://www.bleepingcomputer.com/news/security/dutch-cybersecurity-agency-warns-of-lingering-log4j-risks/)