TellYouThePass Ransomware Exploits Recent PHP RCE Flaw to Breach Servers

Date: 12th June 2024 | Severity: High

Summary

The TellYouThePass ransomware gang has been exploiting the recently patched CVE-2024-4577 remote code execution vulnerability in PHP to deliver webshells and execute the encryptor payload on target systems. The ransomware campaign has been in operation has taken various forms over the years. Recently observed variants have taken the form of .NET samples delivered using HTML applications. TellYouThePass ransomware is known for quickly jumping on public exploits for vulnerabilities with a wide impact. Last November they used an Apache ActiveMQ RCE in attacks.

Attack Vectors

- TellYouThePass ransomware was recently associated with Log4Shell post-exploitation, targeting Windows and Linux
- The TellYouThePass ransomware family was recently reported as a post-exploitation malicious payload used in conjunction with a remote code execution vulnerability in Apache Log4j library, dubbed Log4Shell.
- The initial infection is performed with the use of an HTA file , which contains a malicious VBScript. The VBScript contains a long base64 encoded string, which when decoded reveals bytes of a binary, which are loaded into memory during runtime.
- The malware sends an HTTP request to a command-and-control (C2) server disguised as a CSS resource request and encrypts files on the infected machine. It then places a ransom note, “READ_ME10.html,” with instructions for the victim on how to restore their files.
- TellYouThePass gang to HelloKitty ransomware attacks leveraging the same ActiveMQ vulnerability.
- PHP exploitation campaign, the TellYouThePass ransomware actor continues to demonstrate its ability to incorporate newly disclosed vulnerabilities into its attack toolkit rapidly.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 395279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3 • 5a2b9ddddea96f21d905036761ab27627bd6db4f5973b006f1e39d4acb04a618 • 9562AD2C173B107A2BAA7A4986825B52E881A935DEB4356BF8B80B1EC6D41C53 • 48f1495b4e7801352b56cb7baa5c27a9 • 25753e9136077d46199bfb3fa1311bfd • 6a450113e6b097a0ea07593b7b606790 • 2539b7b9d1b88d613126e9968a52787b
IP	• 88.218.76[.]13 • 107.175.127[.]195
URL	• hxxp:/88.218.76[.]13/dd3.hta

Recommendation

- Be aware of your applications, and patch rising vulnerabilities as soon as possible. Perform regular vulnerability scans and security assessments and promptly update systems and applications to fix known vulnerabilities.
- Leverage products like Imperva's Web Application Firewall to stop attacks minutes after they're discovered in the wild.
- Use Anti-Virus programs to provide a first line of defense against malware campaigns like TellYouThePass. Do not open suspicious or unexpected emails, especially the links and attachments in them. Use antivirus software to scan an unknown file before opening it.
- Download products via official and verified channels, and activate and update products using tools or functions provided by the official developer. Illegal activation tools and third-party downloaders are not recommended, as they are often used to distribute malicious content.
- Web Application Security: Implement strong access controls and authentication mechanisms ,Use Web Application Firewalls (WAFs) to filter malicious traffic. Monitor logs for suspicious activity.
- Network Segmentation: Isolate critical systems from less secure parts of your network. Limit lateral movement for attackers.
- Endpoint Protection: Use reliable antivirus and anti-malware software.Enable behavior-based detection and real-time scanning.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-exploits-recent-php-rce-flaw-to-breach-servers/
- https[:]//cybersecuritynews.com/tellyouthepass-php-rce-flaw/
- https[:]//securityboulevard.com/2024/06/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/