Se ha detectado que varios actores malintencionados están aprovechando una reciente vulnerabilidad de seguridad en PHP para distribuir troyanos de acceso remoto, mineros de criptomonedas y botnets para ataques de denegación de servicio distribuido (DDoS).

La vulnerabilidad en cuestión es CVE-2024-4577 (puntuación CVSS: 9.8), que permite a un atacante ejecutar comandos maliciosos de manera remota en sistemas Windows configurados en los idiomas chino y japonés. Se divulgó públicamente a principios de junio de 2024.

> *«CVE-2024-4577 es una falla que permite a un atacante eludir la línea de comandos y pasar argumentos para ser interpretados directamente por PHP. La vulnerabilidad radica en cómo los caracteres Unicode se convierten en ASCII»*, explicaron los investigadores de Akamai Kyle Lefton, Allen West y Sam Tinklenberg en un análisis realizado el miércoles.

La empresa de infraestructura web informó que comenzó a observar intentos de explotación contra sus servidores honeypot, enfocándose en la falla de PHP dentro de las 24 horas posteriores a su divulgación pública.

Estos intentos de explotación incluyeron el uso de exploits para distribuir un troyano de acceso remoto llamado Gh0st RAT, mineros de criptomonedas como RedTail y XMRig, y un botnet DDoS denominado Muhstik.

> *«El atacante envió una solicitud similar a las otras vistas en operaciones anteriores de RedTail, aprovechando la falla del guion suave con '%ADd' para ejecutar una solicitud wget para un script de shell. Este script realiza una solicitud adicional a la misma dirección IP en Rusia para obtener una versión x86 del malware de minería de criptomonedas RedTail»,* explicaron los investigadores.

El mes pasado, Imperva también reveló que CVE-2024-4577 está siendo explotada por actores del ransomware TellYouThePass para distribuir una variante .NET del malware de cifrado de archivos.

Se recomienda a los usuarios y organizaciones que utilizan PHP actualizar sus instalaciones a la última versión para protegerse contra amenazas activas.

> *«El tiempo cada vez más corto que los defensores tienen para protegerse después de la divulgación de una nueva vulnerabilidad es otro riesgo de seguridad crítico. Esto es especialmente cierto para esta vulnerabilidad de PHP debido a su alta explotabilidad y rápida adopción por parte de los actores malintencionados»,* comentaron los investigadores.

La divulgación se produce mientras Cloudflare informó de un aumento del 20% en los ataques DDoS año tras año en el segundo trimestre de 2024, y que mitigó 8.5 millones de ataques DDoS durante los primeros seis meses. En comparación, la compañía bloqueó 14 millones de ataques DDoS en todo 2023.

> *«En general, el número de ataques DDoS en el segundo trimestre disminuyó un 11% con respecto al trimestre anterior, pero aumentó un 20% interanual»,* informaron los investigadores Omer Yoachimik y Jorge Pacheco en el informe de amenazas DDoS para el segundo trimestre de 2024.

Además, los botnets DDoS conocidos representaron la mitad de todos los ataques HTTP DDoS. Los agentes de usuario falsos y los navegadores sin cabeza (29%), los atributos HTTP sospechosos (13%) y las inundaciones genéricas (7%) fueron los otros vectores prominentes de ataques HTTP DDoS.

El país más atacado durante este período fue China, seguido por Turquía, Singapur, Hong

Kong, Rusia, Brasil, Tailandia, Canadá, Taiwán y Kirguistán. Los sectores de tecnología de la información y servicios, telecomunicaciones, bienes de consumo, educación, construcción y alimentos y bebidas fueron los principales objetivos de los ataques DDoS.

> *«Argentina se clasificó como la mayor fuente de ataques DDoS en el segundo trimestre de 2024. Indonesia le siguió de cerca en segundo lugar, seguida por los Países Bajos en tercer lugar»,* indicaron los investigadores.