Los actores maliciosos probablemente están utilizando exploits de prueba de concepto (PoC) disponibles públicamente para aprovechar vulnerabilidades de seguridad recientemente descubiertas en el software WhatsUp Gold de Progress Software y realizar ataques oportunistas.

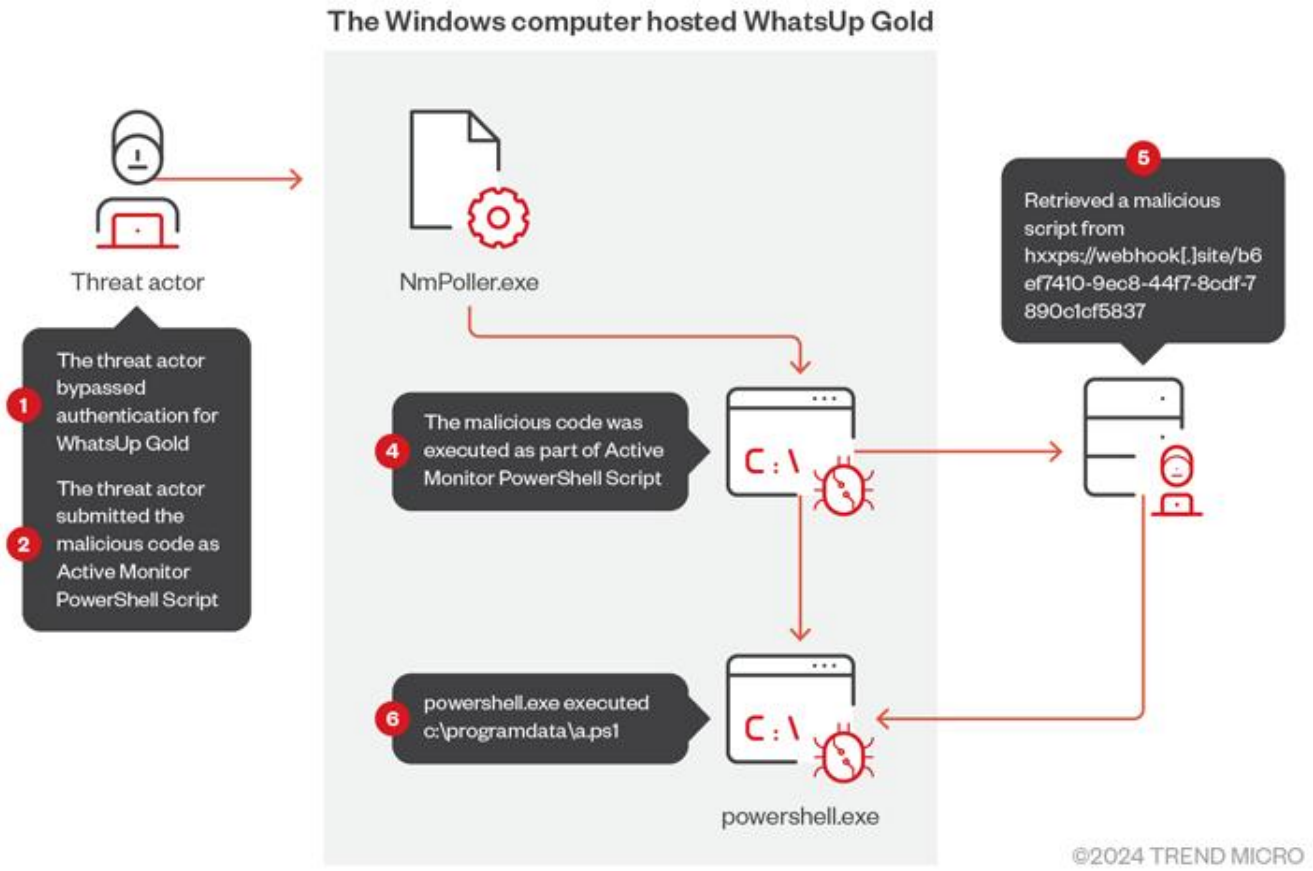
Se informa que la actividad comenzó el 30 de agosto de 2024, apenas cinco horas después de que el investigador de seguridad Sina Kheirkhah, del equipo Summoning Team, publicara un PoC para la vulnerabilidad CVE-2024-6670 (calificación CVSS: 9.8). Kheirkhah también fue quien descubrió y reportó la vulnerabilidad CVE-2024-6671 (calificación CVSS: 9.8).

Ambas fallas críticas, que permiten a un atacante no autenticado obtener la contraseña encriptada de un usuario, fueron corregidas por Progress a mediados de agosto de 2024.

> *«La secuencia de eventos sugiere que, a pesar de que los parches ya estaban disponibles, algunas organizaciones no lograron aplicarlos a tiempo, lo que resultó en incidentes casi de inmediato tras la publicación del PoC»,* explicaron en un análisis realizado el jueves las investigadoras de Trend Micro, Hitomi Kimura y Maria Emreen Viray.

Los ataques detectados por la firma de ciberseguridad implican la elusión de la autenticación en WhatsUp Gold para explotar el Active Monitor PowerShell Script y, eventualmente, descargar varias herramientas de acceso remoto que les permiten mantener el acceso en el sistema Windows comprometido.

Entre las herramientas utilizadas se encuentran Atera Agent, Radmin, SimpleHelp Remote Access y Splashtop Remote, con Atera Agent y Splashtop Remote siendo instalados a través de un único archivo MSI descargado desde un servidor remoto.



«El proceso de sondeo NmPoller.exe, el ejecutable de WhatsUp Gold, parece ser capaz de alojar un script llamado Active Monitor PowerShell Script como una función legítima», señalaron las investigadoras. «Los atacantes aprovecharon esto para ejecutar código arbitrario de forma remota».

Aunque no se han observado acciones adicionales de explotación, el uso de varias herramientas de acceso remoto sugiere la posible implicación de un grupo de ransomware.

Esta es la segunda ocasión en la que se han explotado activamente vulnerabilidades en WhatsUp Gold. A principios del mes pasado, la Fundación Shadowserver informó sobre intentos de explotación dirigidos a la vulnerabilidad CVE-2024-4885 (calificación CVSS: 9.8), otro fallo crítico que Progress solucionó en junio de 2024.

Este anuncio se produce semanas después de que Trend Micro también revelara que actores maliciosos están aprovechando una vulnerabilidad ya parcheada en Atlassian Confluence Data Center y Confluence Server (CVE-2023-22527, calificación CVSS: 10.0) para implantar el web shell Godzilla.

> *«La vulnerabilidad CVE-2023-22527 sigue siendo ampliamente explotada por una variedad de actores de amenazas que se aprovechan de esta falla para realizar actividades maliciosas, lo que la convierte en un riesgo de seguridad considerable para organizaciones a nivel global»,* señaló la compañía.