Una reciente vulnerabilidad corregida en Microsoft Windows Server Update Services (WSUS) ha sido aprovechada por actores maliciosos para distribuir el malware conocido como ShadowPad.

"El atacante se enfocó en servidores Windows con WSUS habilitado, explotando CVE-2025-59287 para obtener acceso inicial," señaló el AhnLab Security Intelligence Center (ASEC) en un informe publicado la semana pasada. *"Luego emplearon PowerCat, una herramienta de PowerShell basada en Netcat y de código abierto, para obtener una shell del sistema (CMD). Posteriormente, descargaron e instalaron ShadowPad utilizando certutil y curl."*

ShadowPad, considerado el sucesor de PlugX, es una puerta trasera modular ampliamente empleada por grupos de ciberespionaje patrocinados por el Estado chino. Surgió por primera vez en 2015. En un análisis publicado en agosto de 2021, SentinelOne lo calificó como *"una obra maestra de malware vendido de forma privada dentro del espionaje chino."*

CVE-2025-59287, corregido por Microsoft el mes pasado, corresponde a una falla crítica de deserialización en WSUS que podría permitir la ejecución remota de código con privilegios de sistema. La vulnerabilidad ha sido objeto de una explotación intensa, ya que los atacantes la han usado para obtener acceso inicial a instancias de WSUS expuestas públicamente, realizar reconocimiento e incluso desplegar herramientas legítimas como Velociraptor.

Target Type	File Name	File Size	File Path
Parent	wsusservice.exe	17 KB	%ProgramFiles%\update services\services\wsusservice.exe
Target	certutil.exe	1.58 MB	%SystemRoot%\system32\certutil.exe
Current	cmd.exe	272 KB	%SystemRoot%\system32\cmd.exe

Process	Target	Behavior	Data
cmd.exe	certutil.exe	Creates process	N/A
cmd.exe	etdctrlhelper.exe	Creates process	N/A
certutil.exe	N/A	Creates executable file	etdapix.dll

En el ataque documentado por la empresa surcoreana de ciberseguridad, se observó que los atacantes aprovecharon la falla para ejecutar utilidades de Windows como *«curl.exe»* y *«certutil.exe»* a fin de conectarse con un servidor externo (*«149.28.78[.]189:42306»*) y así descargar e instalar ShadowPad.

ShadowPad, al igual que PlugX, se ejecuta mediante la técnica de carga lateral de DLL, utilizando un binario legítimo (*«ETDCtrlHelper.exe»*) para activar una DLL maliciosa (*«ETDApix.dll»*), la cual funciona como un cargador residente en memoria para iniciar la puerta trasera.

Una vez implantado, el malware ejecuta un módulo principal responsable de cargar en memoria otros complementos incluidos en el shellcode. También incorpora múltiples técnicas de persistencia y evasión. Hasta el momento, esta actividad no ha sido atribuida a ningún actor o grupo de amenazas conocido.

"Tras la publicación del código de explotación proof-of-concept (PoC) para esta vulnerabilidad, los atacantes lo armaron rápidamente para distribuir ShadowPad mediante servidores WSUS," indicó AhnLab. *"Esta vulnerabilidad es crítica porque permite la ejecución remota de código con permisos a nivel de sistema, incrementando significativamente el*

impacto potencial.”