La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha identificado un nuevo malware llamado RESURGE, el cual ha sido utilizado en ataques que explotan una vulnerabilidad de seguridad en los dispositivos Ivanti Connect Secure (ICS). Esta vulnerabilidad ya ha sido corregida.

Características de RESURGE
Según CISA, RESURGE comparte funcionalidades con la variante de malware SPAWNCHIMERA, incluyendo la capacidad de persistir tras reinicios. Sin embargo, RESURGE introduce comandos específicos que modifican su comportamiento. Este malware posee características avanzadas, actuando como rootkit, dropper, puerta trasera (backdoor), bootkit, proxy y herramienta de túnel.

Vulnerabilidad explotada: CVE-2025-0282
RESURGE se aprovecha de la vulnerabilidad CVE-2025-0282, que es un desbordamiento de búfer basado en pila en Ivanti Connect Secure, Policy Secure y ZTA Gateways. Esta falla permite la ejecución remota de código y afecta las siguientes versiones:

- Ivanti Connect Secure anterior a la versión 22.7R2.5
- Ivanti Policy Secure anterior a la versión 22.7R1.2
- Ivanti Neurons for ZTA Gateways anterior a la versión 22.7R2.3

Conexión con grupos de amenazas
Investigadores de Mandiant, propiedad de Google, han identificado que esta vulnerabilidad ha sido aprovechada para distribuir un conjunto de malwares conocidos como SPAWN, que incluye SPAWNANT, SPAWNMOLE y SPAWNSNAIL. Este ecosistema de malware ha sido vinculado al grupo de espionaje UNC5337, con conexiones a China.

Recientemente, JPCERT/CC informó que se ha utilizado esta vulnerabilidad para desplegar una versión mejorada de SPAWN, llamada SPAWNCHIMERA, que unifica múltiples módulos en un solo malware y facilita la comunicación entre procesos mediante sockets de dominio UNIX. Además, esta variante es capaz de parchear CVE-2025-0282 para evitar que otros actores maliciosos lo exploten.

Mejoras de RESURGE

Según CISA, RESURGE (identificado como «libdsupgrade.so») es una versión avanzada de SPAWNCHIMERA e introduce tres nuevos comandos:

1. Insertarse en «ld.so.preload», instalar una web shell, modificar verificaciones de integridad y alterar archivos.
2. Habilitar web shells para el robo de credenciales, creación de cuentas, restablecimiento de contraseñas y escalamiento de privilegios.
3. Copiar la web shell en el disco de arranque de Ivanti y modificar la imagen en ejecución de coreboot.

Además, CISA encontró dos artefactos adicionales en un dispositivo ICS de una entidad de infraestructura crítica:

- Una variante de SPAWNSLOTH («liblogblock.so») dentro de RESURGE, diseñada para alterar los registros del sistema de los dispositivos Ivanti.
- Un binario personalizado ELF de 64 bits («dsmain») que contiene un script de shell y componentes del conjunto de herramientas BusyBox. Este script permite extraer una imagen de kernel descomprimida (vmlinux) de un sistema comprometido.

Amenaza persistente

Microsoft ha revelado que la vulnerabilidad CVE-2025-0282 también ha sido explotada como un ataque de día cero por otro grupo vinculado a China, identificado como Silk Typhoon (anteriormente conocido como Hafnium).

Recomendaciones de seguridad

Debido a la evolución constante de estos ataques, CISA recomienda a las organizaciones actualizar sus dispositivos Ivanti a las versiones más recientes. Adicionalmente, se aconseja:

- Restablecer las credenciales de cuentas privilegiadas y no privilegiadas.
- Rotar las contraseñas de todos los usuarios de dominio y cuentas locales.
- Revisar y ajustar políticas de acceso, restringiendo temporalmente privilegios en

dispositivos afectados.
- Monitorizar cuentas en busca de actividad inusual.