Ivanti ha emitido una advertencia sobre una vulnerabilidad crítica de seguridad que está siendo explotada activamente, la cual afecta a Ivanti Connect Secure, Policy Secure y ZTA Gateways desde mediados de diciembre de 2024.

La vulnerabilidad en cuestión es CVE-2025-0282 (con un puntaje CVSS de 9.0), un desbordamiento de búfer basado en pila que impacta a Ivanti Connect Secure antes de la versión 22.7R2.5, Ivanti Policy Secure antes de la versión 22.7R1.2, e Ivanti Neurons para ZTA Gateways antes de la versión 22.7R2.3.

> Ivanti explicó en su aviso que *«la explotación exitosa de CVE-2025-0282 podría permitir la ejecución remota de código sin autenticación. La actividad del actor de amenazas fue detectada por la herramienta de verificación de integridad (ICT) el mismo día que ocurrió, lo que permitió a Ivanti responder rápidamente y desarrollar una solución».*

La empresa también ha corregido otra vulnerabilidad crítica (CVE-2025-0283, con un puntaje CVSS de 7.0), que permite a un atacante autenticado localmente escalar sus privilegios. Estas vulnerabilidades fueron abordadas en la versión 22.7R2.5 y afectan las siguientes versiones:

- CVE-2025-0282: Ivanti Connect Secure 22.7R2 hasta 22.7R2.4, Ivanti Policy Secure 22.7R1 hasta 22.7R1.2, e Ivanti Neurons para ZTA Gateways 22.7R2 hasta 22.7R2.3
- CVE-2025-0283: Ivanti Connect Secure 22.7R2.4 y versiones anteriores, 9.1R18.9 y versiones anteriores, Ivanti Policy Secure 22.7R1.2 y versiones anteriores, e Ivanti Neurons para ZTA Gateways 22.7R2.3 y versiones anteriores

Ivanti ha confirmado estar al tanto de un *«número limitado de clientes»* cuyos dispositivos han sido comprometidos debido a la vulnerabilidad CVE-2025-0282, aunque no hay pruebas de que CVE-2025-0283 esté siendo explotada activamente.

Mandiant, una empresa de ciberseguridad propiedad de Google, que ha investigado los

ataques que explotan CVE-2025-0282, informó sobre el uso del ecosistema de malware SPAWN en dispositivos comprometidos de diversas organizaciones. SPAWN ha sido vinculado a un actor de amenazas asociado a China, denominado UNC5337, que se cree forma parte del grupo UNC5221 con un nivel de confianza medio.

Además, los ataques resultaron en la instalación de familias de malware previamente desconocidas, denominadas DRYHOOK y PHASEJAM. Ninguna de estas familias de malware ha sido vinculada a un actor de amenazas o grupo específico.

La explotación de CVE-2025-0282, según los expertos en ciberseguridad, implica llevar a cabo varios pasos para desactivar SELinux, impedir el reenvío de syslog, montar el disco en modo lectura-escritura, ejecutar scripts para instalar web shells, usar sed para eliminar registros específicos en los archivos de depuración y aplicación, volver a habilitar SELinux y montar nuevamente el disco.

Uno de los payloads ejecutados a través de un script de shell es otro script que, a su vez, ejecuta un binario ELF encargado de activar PHASEJAM, un instalador de scripts que realiza cambios maliciosos en los componentes del dispositivo Ivanti Connect Secure.

> *«Las funciones principales de PHASEJAM incluyen insertar un web shell en los archivos getComponent.cgi y restAuth.cgi, bloquear las actualizaciones del sistema mediante la modificación del archivo DSUpgrade.pm, y sobrescribir el ejecutable remotedebug para que pueda usarse para ejecutar comandos arbitrarios cuando se pase un parámetro específico»*, indicaron los investigadores de Mandiant.

El web shell tiene la capacidad de decodificar comandos de shell y exfiltrar los resultados de la ejecución de los mismos, cargar archivos arbitrarios en el dispositivo comprometido y leer y transmitir los contenidos de archivos.

Existen indicios de que el ataque fue realizado por un actor de amenazas sofisticado, dado que se han eliminado de forma meticulosa entradas de registro, mensajes del núcleo, trazas

de fallos, errores en el manejo de certificados e historial de comandos.

PHASEJAM también garantiza la persistencia al bloquear de manera encubierta las actualizaciones legítimas del dispositivo Ivanti, mostrando una falsa barra de progreso de actualización en HTML. Por otro lado, SPAWNANT, el componente instalador del marco de malware SPAWN, puede persistir durante las actualizaciones del sistema al secuestrar el flujo de ejecución de dspkginstall, un binario usado en el proceso de actualización.

Mandiant también observó el uso de diversas herramientas de túneles, como SPAWNMOLE, que permiten la comunicación entre el dispositivo comprometido y la infraestructura de comando y control (C2) del actor de amenazas.

Otras actividades posteriores a la explotación incluyen:

- Realizar un análisis de la red interna utilizando herramientas como nmap y dig
- Utilizar la cuenta de servicio LDAP para realizar consultas y moverse lateralmente dentro de la red, incluidos los servidores de Active Directory, a través de SMB o RDP
- Robar bases de datos de caché de aplicaciones que contienen información de sesiones VPN, cookies, claves API, certificados y credenciales
- Desplegar un script en Python llamado DRYHOOK para robar credenciales

Mandiant también advirtió que es posible que varios grupos de hackers sean responsables de la creación y distribución de SPAWN, DRYHOOK y PHASEJAM, aunque señaló que no tiene suficiente información para estimar con precisión el número de actores de amenazas involucrados en la explotación de la vulnerabilidad.

Debido a la explotación activa de la vulnerabilidad, la Agencia de Ciberseguridad y Seguridad de Infraestructura de los EE. UU. (CISA) ha incluido CVE-2025-0282 en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), exigiendo que las agencias federales apliquen los parches correspondientes antes del 15 de enero de 2025. Además, está instando a las organizaciones a revisar sus entornos en busca de signos de compromiso y a reportar cualquier incidente o actividad sospechosa.

Actualización

Ivanti sugiere utilizar la herramienta Integrity Checker Tool (ICT) para detectar posibles casos de explotación relacionados con la vulnerabilidad CVE-2025-0282. En caso de identificar actividad sospechosa, se recomienda realizar un restablecimiento de fábrica en el dispositivo para eliminar cualquier malware presente y luego restaurarlo a producción utilizando la versión 22.7R2.5.

La compañía también enfatizó que los dispositivos Policy Secure no están diseñados para tener acceso directo a internet. «Las puertas de enlace Ivanti Neurons ZTA no son vulnerables a explotación mientras están en uso en producción», declaró la empresa. «Sin embargo, si se crea una puerta de enlace para esta solución y no se conecta a un controlador ZTA, podría existir un riesgo de explotación en dicha puerta de enlace generada».