Una operación de gran escala enfocada en el robo de credenciales ha sido detectada aprovechando la vulnerabilidad React2Shell como punto inicial de infección, con el objetivo de sustraer credenciales de bases de datos, claves privadas SSH, secretos de Amazon Web Services (AWS), historial de comandos de shell, claves API de Stripe y tokens de GitHub de forma masiva.

Cisco Talos ha atribuido esta actividad a un grupo de amenazas identificado como UAT-10608. Como parte de esta campaña, al menos 766 sistemas distribuidos en distintas regiones geográficas y proveedores de nube han sido comprometidos.

"Tras lograr el acceso inicial, UAT-10608 utiliza scripts automatizados para extraer y exfiltrar credenciales de múltiples aplicaciones, las cuales posteriormente son enviadas a su infraestructura de comando y control (C2)", señalaron los investigadores de seguridad Asheer Malhotra y Brandon White en un informe.

"El servidor C2 aloja una interfaz gráfica basada en web denominada 'NEXUS Listener', que permite visualizar la información robada y obtener análisis mediante estadísticas precompiladas sobre las credenciales recolectadas y los sistemas comprometidos."

Se estima que la campaña está dirigida a aplicaciones Next.js vulnerables a CVE-2025-55182 (puntaje CVSS: 10.0), una falla crítica en los componentes React Server Components y el enrutador de aplicaciones de Next.js que podría permitir la ejecución remota de código. A partir de este acceso inicial, los atacantes despliegan el framework de recolección NEXUS Listener.

Esto se lleva a cabo mediante un dropper que instala un script de extracción en múltiples fases, el cual recopila diversos datos del sistema comprometido, tales como:

- Variables de entorno
- Entorno procesado en formato JSON desde el runtime de JavaScript
- Claves privadas SSH y archivos authorized_keys
- Historial de comandos de shell

- Tokens de cuentas de servicio de Kubernetes
- Configuraciones de contenedores Docker (contenedores activos, imágenes, puertos expuestos, redes, puntos de montaje y variables de entorno)
- Claves API
- Credenciales temporales asociadas a roles IAM mediante consultas al servicio de metadatos de instancias en AWS, Google Cloud y Microsoft Azure
- Procesos en ejecución

La compañía de ciberseguridad indicó que el amplio espectro de víctimas y el patrón de ataque no selectivo sugieren el uso de escaneos automatizados, probablemente apoyados en servicios como Shodan, Censys o herramientas propias, para detectar implementaciones públicas de Next.js y evaluar su vulnerabilidad.

En el núcleo del framework se encuentra una aplicación web protegida por contraseña que permite al operador acceder a todos los datos robados mediante una interfaz gráfica con funciones de búsqueda para analizar la información.

"La aplicación muestra diversas estadísticas, incluyendo el número de sistemas comprometidos y el total de cada tipo de credencial extraída con éxito", explicó Talos. *"También permite explorar cada uno de los sistemas afectados y muestra el tiempo de actividad de la propia aplicación."*

La versión actual de NEXUS Listener es la V3, lo que indica que la herramienta ha pasado por múltiples iteraciones de desarrollo antes de alcanzar su estado actual.

Talos, que logró acceder a datos de una instancia de NEXUS Listener sin autenticación, señaló que contenía claves API vinculadas a Stripe, plataformas de inteligencia artificial (OpenAI, Anthropic y NVIDIA NIM), servicios de comunicación (SendGrid y Brevo), además de tokens de bots de Telegram, secretos de webhooks, tokens de GitHub y GitLab, cadenas de conexión a bases de datos y otros secretos de aplicaciones.

La magnitud de la recolección de datos pone de manifiesto cómo los atacantes pueden

aprovechar sistemas comprometidos para preparar ataques posteriores. Se recomienda a las organizaciones auditar sus entornos, aplicar el principio de privilegio mínimo, habilitar el escaneo de secretos, evitar reutilizar pares de claves SSH, implementar IMDSv2 en todas las instancias AWS EC2 y rotar credenciales en caso de sospecha de compromiso.

"Más allá del valor operativo inmediato de cada credencial, el conjunto total de datos representa un mapa detallado de la infraestructura de las organizaciones afectadas: qué servicios utilizan, cómo están configurados, qué proveedores de nube emplean y qué integraciones con terceros tienen implementadas", indicaron los investigadores.

"Esta información resulta extremadamente valiosa para diseñar ataques dirigidos posteriores, campañas de ingeniería social o incluso para vender accesos a otros actores maliciosos."