GitHub ha anunciado una mejora en su función de detección de secretos que amplía las comprobaciones de validez a servicios populares como Amazon Web Services (AWS), Microsoft, Google y Slack.

Las comprobaciones de validez, introducidas por la subsidiaria de Microsoft a principios de este año, notifican a los usuarios si los tokens expuestos detectados por la detección de secretos están activos, lo que permite tomar medidas eficaces para remediarlos. Inicialmente, esta funcionalidad se habilitó solo para los tokens de GitHub.

El servicio de alojamiento de código y control de versiones en la nube mencionó que tiene la intención de admitir más tokens en el futuro.

Para activar esta configuración, los propietarios de empresas u organizaciones y los administradores de repositorios pueden dirigirse a Configuración > Seguridad y análisis de código > Detección de secretos y marcar la opción *«Verificar automáticamente si un secreto es válido enviándolo al socio correspondiente».*

A principios de este año, GitHub también amplió las alertas de detección de secretos para todos los repositorios públicos y anunció la disponibilidad de protección contra envíos para ayudar a los desarrolladores y mantenedores a asegurar proactivamente su código al buscar secretos altamente identificables antes de que se realicen los envíos.

Este desarrollo coincide con el anuncio de Amazon de requisitos mejorados de protección de cuentas que obligarán a los usuarios privilegiados (también conocidos como usuarios root) de una cuenta de AWS Organization a habilitar la autenticación multifactor (MFA) a partir de mediados de 2024.

> *«MFA es una de las formas más sencillas y efectivas de mejorar la seguridad de una cuenta, ya que ofrece una capa adicional de protección para prevenir que individuos no autorizados accedan a sistemas o datos»,* declaró Steve Schmidt, director de seguridad de Amazon.

Métodos de MFA débiles o mal configurados también se encuentran entre las 10 configuraciones de red más comunes, según un nuevo aviso conjunto emitido por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).

> *«Algunos tipos de MFA son vulnerables a ataques de phishing, 'push bombing', explotación de vulnerabilidades del protocolo Signaling System 7 (SS7) y/o técnicas de 'intercambio de SIM'»,* señalaron las agencias.

> *«Estos intentos, si tienen éxito, pueden permitir que un actor de amenazas obtenga acceso a credenciales de autenticación MFA o evada MFA y acceda a sistemas protegidos por MFA».*

Entre otras configuraciones de ciberseguridad prevalentes se encuentran:

- Configuraciones predeterminadas de software y aplicaciones.
- Separación inadecuada de privilegios de usuario/administrador.
- Monitorización interna insuficiente de la red.
- Falta de segmentación de red.
- Gestión deficiente de parches.
- Elusión de controles de acceso al sistema.
- Listas de control de acceso (ACL) insuficientes en recursos compartidos y servicios de red.
- Higiene de credenciales deficiente.
- Ejecución de código sin restricciones.

Como medidas de mitigación, se recomienda que las organizaciones eliminen las credenciales predeterminadas y refuercen las configuraciones; desactiven servicios no utilizados e implementen controles de acceso; den prioridad a la aplicación de parches;

realicen auditorías y supervisen cuentas administrativas y privilegios.

También se insta a los proveedores de software a implementar principios de diseño seguro, utilizar lenguajes de programación seguros en la memoria cuando sea posible, evitar contraseñas predeterminadas, proporcionar registros de auditoría de alta calidad a los clientes sin costo adicional y exigir métodos de MFA resistentes al phishing.

> *«Estas configuraciones erróneas ilustran (1) una tendencia de debilidades sistémicas en muchas organizaciones grandes, incluso aquellas con posturas maduras de ciberseguridad, y (2) la importancia de que los fabricantes de software adopten principios de diseño seguro para reducir la carga sobre los defensores de la red»,* señalaron las agencias.