CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Acceso No Autorizado

Fecha: 03/01/2023

Problemática: Exfiltración de Código Fuente Dropbox Desk Tools

Correlativo: AC-0002

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Drupobox emitió un comunicado a través de sus canales oficiales para informar a sus usuarios sobre la exfiltración de código fuente que un actor de amenazas llevo a cabo a través de la plataforma GitHub.

SITUACIÓN

Dropbox reveló una brecha de seguridad después de que ciberdelincuentes robaran 130 repositorios de códigos después de obtener acceso a una de sus cuentas de GitHub usando las credenciales de los empleados robadas en un ataque de phishing.

La filtración exitosa fue el resultado de un ataque de phishing que apuntó a varios empleados de Dropbox utilizando correos electrónicos que se hacían pasar por la plataforma de entrega e integración continua de CircleCI. El ataque los redirigió a una página de inicio de phishing donde se les pidió que ingresaran su nombre de usuario y contraseña de GitHub. En la misma página de phishing, también se les pidió a los empleados que "usaran su clave de autenticación de hardware para pasar una contraseña de un solo uso (OTP)".

El actor de amenaza llevo a cabo el ataque utilizando la técnica T1566 según Mitre Attack

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alta**	**Alta**	**Alta**

RECOMENDACIONES

- Habilitar la autenticación de dos factores en tu cuenta para que el acceso requiera algo más que una contraseña.
- Revisar las claves SSH , implementar claves e integraciones autorizadas y revocar el acceso no autorizado o desconocido en las configuraciones de SSH y aplicaciones.
- Verificar todas las direcciones de correo electrónico . Si un atacante agregó su dirección de correo electrónico a tu cuenta, podría permitirle forzar un restablecimiento de contraseña no deseado.
- Revisar el registro de seguridad de tu cuenta . Esto proporciona una descripción general de varias configuraciones realizadas en tus repositorios. Por ejemplo, puedes asegurarte de que ningún repositorio privado se haya convertido en público o que no se haya transferido ningún repositorio.
- Revisar los webhooks en tus repositorios. Los webhooks podrían permitir que un atacante intercepte las inserciones realizadas en tu repositorio.
- Asegúrate de que no se crearon nuevas claves de implementación. Esto podría permitir el acceso de servidores externos a tus proyectos.
- Revisar las confirmaciones recientes realizadas en tus repositorios.

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo y filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).

REFERENCIAS

1. https://nvd.nist.gov/vuln/detail/CVE-2022-35842
2. https://hackwise.mx/dropbox-revela-que-hackers-le-robaron-130-repositorios-de-github-con-codigo-fuente/?fbclid=IwAR2YamUVIII_ASJC7qVpd7CELa0X15TJp40DwR-G6FqLq5J7dEOAKoHVq90
3. https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox
4. https://attack.mitre.org/techniques/T1566/