Vulnerabilidad En Google Apps Permite El Robo De Cuentas

Se ha conocido una vulnerabilidad crítica de cross-site scripting (XSS) en la consola de administrador de Google Apps, la cual permite a los atacantes obligar a los administradores de Google Apps ejecutar casi cualquier solicitud en el dominio **https:/admin.google.com**.

La **consola de administración de Google Apps** permite a los administradores gestionar la cuenta de su organización. Los administradores pueden utilizar la consola para añadir nuevos usuarios, configurar permisos, administrar la configuración de seguridad y permitir los servicios de Google.

La función se utiliza principalmente por muchas empresas, especialmente los que utilizan **Gmail como el servicio de correo electrónico** para su dominio.

La vulnerabilidad XSS permite a los atacantes obligar al administrador realizar las siguientes acciones:

- Creación de nuevos usuarios con derechos de «super» administrador
- Desactivación de la autenticación de dos factores y otras medidas de seguridad de las cuentas existentes o de varios dominios
- Modificación de la configuración de dominio para que todos los correos electrónicos entrantes se redirijan a direcciones controladas por el atacante
- Secuestrar una cuenta / correo electrónico de restablecimiento de la contraseña, la desactivación de la autenticacion de 2 pasos.

Esta nueva vulnerabilidad de Zero Day se descubrió e informó de forma privada por el ingeniero de seguridad de aplicaciones Brett Buerhaus a Google el 1 de septiembre del año pasado, y

la empresa solucionó el defecto en los siguientes 17 días. A cambio de este informe, Google pagó el investigador 5.000 dólares como recompensa conforme a su **programa de recompensas de errores**.

Según el investigador, cuando los usuarios acceden a un servicio que no se ha configurado para su dominio, pueden visualizar una página «ServiceNotAllowed». Esta página permite a los usuarios cambiar entre las diferentes cuentas asociadas, con el fin de iniciar sesión en el servicio.

Sin embargo, cuando se selecciona una de las cuentas, un **fragmento de código JavaScript** se ejecuta en un intento de redirigir el navegador web del usuario. Este código JavaScript podría ser suministrado por el usuario en la solicitud para»continuar», lo cual permite este **ataque de XSS**.

> *«El parámetro de la petición a seguir es bastante diferente de la petición común en el flujo de acceso a Google,» Buerhaus explicó en su blog publicado el miércoles. «. Esta es la única página que he podido encontrar que no valida la URL pasada. Esto permitió a los ataques de cross-site scripting usando javascript como parte de la URL y se ejecutaría cuando la ubicación del navegador es redirigida «.*

Solucionar la vulnerabilidad a los 17 días luego de haber informado a la empresa muestra la preocupación por la búsqueda de soluciones para los usuarios por parte del gigante de las búsquedas. Esto es bastante bueno en comparación a Microsoft, recordemos que hace poco el equipo de Project Zero encontró el tercer fallo de seguridad, aun no habiendo solucionado las anteriores vulnerabilidades.