



RubyGems hace que la autenticación multifactor sea obligatoria para los principales mantenedores de paquetes

RubyGems, el administrador de paquetes oficial para el lenguaje de programación Ruby, se ha convertido en la última plataforma en exigir la autenticación multifactor (MFA) para los mantenedores de paquetes populares, siguiendo los pasos de [NPM](#) y PyPI.

Con ese fin, los propietarios de gemas con más de 180 millones de descargas totales deben activar MFA a partir del 15 de agosto de 2022.

«Los usuarios de esta categoría que no tengan la MFA habilitada en la interfaz de usuario y la API o en el nivel de inicio de sesión de la interfaz de usuario y gema no podrán editar su perfil en la web, realizar acciones privilegiadas (es decir, empujar y extraer gemas, o agregar y eliminar propietarios de gemas) o iniciar sesión en la línea de comando hasta que configuren MFA», [dijo RubyGems](#).

Además, se espera que los mantenedores de gemas que superen los 165 millones de descargas acumuladas reciban recordatorios para activar MFA hasta que el conteo de descargas alcance los 180 millones de umbrales, momento en el que será obligatorio.

El desarrollo se ve como un intento de los ecosistemas de paquetes para reforzar la cadena de suministro de software y evitar ataques de apropiación de cuentas, lo que podría permitir a los atacantes aprovechar el acceso para enviar paquetes no autorizados a los clientes intermedios.

El nuevo requisito también surge en un contexto en el que los adversarios ponen cada vez más su mirada en los repositorios de código fuente abierto, con ataques NPM y PyPI creciendo exageradamente en un 289% combinado desde 2018, según un [nuevo análisis de ReversingLabs](#).

En lo que ahora se ha convertido en un tema recurrente, los investigadores de [Checkmarx](#), [Kaspersky](#) y [Snyk](#), descubrieron una gran cantidad de paquetes maliciosos en PyPI que podrían ser objeto de abuso para realizar ataques DDoS y recopilar contraseñas del navegador, así como credenciales e información de pago de Discord y Roblox.