Los encargados del mantenimiento del administrador de paquetes RubyGems, abordaron una vulnerabilidad de seguridad crítica que podría haberse pausado para eliminar gemas y reemplazarlas con versiones no autorizadas en circunstancias específicas.

> *«Debido a un error en la acción yank, era posible que cualquier usuario de RubyGems.org eliminara y reemplazara ciertas gemas incluso si ese usuario no estaba autorizado para hacerlo»*, dijo RubyGems en un aviso de seguridad.

RubyGems, como npm para JavaScript y pip para Python, es un administrador de paquetes y un servicio de alojamiento de gemas para el lenguaje de programación Ruby, que ofrece un repositorio de más de 171,500 bibliotecas.

La falla en cuestión, rastreada como CVE-2022-29176, permitía a cualquiera extraer ciertas gemas y cargar distintos archivos con el mismo nombre, el mismo número de versión y diferentes plataformas.

Sin embargo, para que esto suceda, una gema debía tener uno o más guiones en su nombre, donde la palabra antes del guion era el nombre de una gema controlada por el atacante, y que se creó dentro de los 30 días o no tuvo actualizaciones durante más de 100 días.

> *«Por ejemplo, el propietario de la gema 'something-provider' podría haberse apoderado de la gema 'something'»,* dijeron los propietarios del proyecto.

Los mantenedores del proyecto dijeron que no existe evidencia de que la vulnerabilidad haya sido explotada en la naturaleza, y agregaron que no recibieron ningún correo electrónico de soporte de los propietarios de gemas alertándolos sobre la eliminación de las bibliotecas sin autorización.

> *«Una auditoría de los cambios de gemas durante los últimos 18 meses no encontró ningún ejemplo de que esta vulnerabilidad se use de forma maliciosa. Se está llevando a cabo una auditoría más profunda para cualquier posible uso de este exploit»,* dijeron los mantenedores.

La divulgación se produce cuando NPM abordó varias fallas en su plataforma que podrían haberse convertido en armas para facilitar los ataques de apropiación de cuentas y publicar paquetes maliciosos.

La principal de ellas es una amenaza en la cadena de suministro llamada plantación de paquetes, que permite a los atacantes hacer pasar bibliotecas no autorizadas como legítimas simplemente asignándolas a mantenedores populares y confiables sin su conocimiento.