Matrix, la organización responsable de un proyecto de código abierto que ofrece un protocolo para la comunicación segura y descentralizada en tiempo real, sufrió un ataque cibernético masivo luego de que atacantes desconocidos obtuvieran acceso a los servidores que alojan su sitio web oficial y datos.

Los hackers modificaron el sitio web de Matrix y también robaron mensajes privados sin cifrar, hashes de contraseña, tokens de acceso y claves GPG que los encargados del proyecto utilizaron para firmar paquetes.

El ataque cibernético obligó a la organización a cerrar toda su infraestructura de producción durante varias horas y desconectar a todos los usuarios de Matrix.org.

Así que si tienes una cuenta con el servicio Matrix.org y no cuentas con copias de seguridad, lamentablemente has perdido todos el historial de conversaciones cifradas.

Matrix es un protocolo de mensajería encriptada de código abierto de extremo a extremo que permite que cualquiera pueda auto hospedar un servicio de mensajería en sus propios servidores, alimentando a muchos mensajeros instantáneos, VoIP, WebRTC, bots y comunicación IoT.

Jenkins vulnerable permitió a los hackers acceder al servidor

Según un comunicado de prensa, los atacantes desconocidos explotaron una vulnerabilidad de desvío de sandbox en su infraestructura de producción el 4 de abril, que se ejecutaba en una versión obsoleta y vulnerable del servidor de automatización Jenkins.

La falla de Jenkins permitió a los hackers robar claves SSH internas, que utilizaban para acceder a la infraestructura de producción de Matrix, y finalmente les otorgó acceso a contenido no cifrado, incluidos mensajes personales, hashes de contraseña y tokens de acceso.

JaikeySarra informó la vulnerabilidad el 9 de abril, luego de eso, Matrix identificó el alcance

completo del ataque y eliminó el vulnerable servidor Jenkins, así como la revocación del acceso del atacante desde sus servidores el pasado 10 de abril.

Al siguiente día, Matrix.org también tomó su servidor doméstico y comenzó a reconstruir su infraestructura de producción desde cero, que ahora ha vuelto a estar en línea.

Hoy, aproximadamente a las 5 am UTC, los atacantes también lograron volver a colocar DNS para matrix.org en un sitio web de desfiguración alojado en GitHub usando una clave API de Cloudflare, que se vio comprometida en el ataque y se reemplazó teóricamente durante la reconstrucción.

Debido a que la última modificación confirma que los hash de contraseña encriptados robados se eliminaron de la base de datos de producción, Matrix.org se vio obligado a cerrar la sesión de todos sus usuarios y les aconsejó cambiar sus contraseñas de inmediato.

> *«Esta fue una decisión difícil de tomar. Sopesamos el riesgo de que algunos usuarios pierdan el acceso a los mensajes cifrados contra el de que todas las cuentas de los usuarios son vulnerables al secuestro por medio de los tokens de acceso comprometidos. Esperamos que pueda ver por qué tomamos la decisión de priorizar la integridad de la cuenta sobre el acceso a los mensajes cifrados, pero lamentamos los inconvenientes que esto pueda haber causado»,* dijo la compañía.

La compañía también confirmó que las claves GPG utilizadas para firmar paquetes también se vieron comprometidas, pero afortunadamente, los atacantes no lo usaron para lanzar versiones maliciosas del software firmado con las claves robadas.

Matrix asegura que ambas claves han sido revocadas. Los encargados del proyecto también informaron que pronto comenzarán a enviar por correo electrónico a todos los usuarios afectados para informarles sobre el incidente y aconsejarles que cambien sus contraseñas.