Nuevos descubrimientos arrojan luz sobre lo que se considera un esfuerzo legal para clandestinamente interceptar el tráfico que emana de jabber[.]ru (también conocido como xmpp[.]ru), un servicio de mensajería instantánea basado en XMPP, a través de servidores alojados en Hetzner y Linode (una filial de Akamai) en Alemania.

Un investigador de seguridad que se identifica con el seudónimo ValdikSS afirmó a principios de esta semana: *«El atacante ha generado varios certificados TLS nuevos utilizando el servicio Let's Encrypt, los cuales se utilizaron para tomar el control de las conexiones STARTTLS encriptadas en el puerto 5222 mediante un proxy [hombre en el medio] transparente».*

El ataque se descubrió debido al vencimiento de uno de los certificados MiTM, que no se renovaron.

Las siguientes versiones de BIG-IP se han encontrado vulnerables:

- 17.1.0 (Corregido en 17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG)
- 16.1.0 – 16.1.4 (Corregido en 16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG)
- 15.1.0 – 15.1.10 (Corregido en 15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG)
- 14.1.0 – 14.1.5 (Corregido en 14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG)
- 13.1.0 – 13.1.5 (Corregido en 13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG)

Como medida de mitigación, F5 también proporcionó un script de shell para los usuarios de las versiones 14.1.0 y posteriores de BIG-IP. *«Este script no debe utilizarse en ninguna versión de BIG-IP anterior a 14.1.0, o impedirá que se inicie la utilidad de configuración»*, advirtió la compañía.

Las pruebas reunidas hasta ahora apuntan a que la redirección del tráfico está configurada en la red del proveedor de alojamiento, descartando otras posibilidades, como una violación del servidor o un ataque de suplantación.

Se estima que la interceptación pudo haber durado hasta seis meses, desde el 18 de abril

hasta el 19 de octubre, aunque se ha confirmado que tuvo lugar al menos desde el 21 de julio de 2023 hasta el 19 de octubre de 2023.

Los signos de actividad sospechosa se detectaron por primera vez el 16 de octubre de 2023, cuando uno de los administradores UNIX del servicio recibió un mensaje que indicaba *«El certificado ha caducado»* al conectarse al mismo.

Se cree que el actor de amenazas detuvo la actividad después de que comenzara la investigación sobre el incidente de MiTM el 18 de octubre de 2023. No está claro de inmediato quién está detrás del ataque, pero se sospecha que se trata de una interceptación legal basada en una solicitud de la policía alemana.

Otra teoría, aunque poco probable pero no imposible, es que el ataque de MiTM sea una intrusión en las redes internas de tanto Hetzner como Linode, apuntando específicamente a jabber[.]ru.

> *«Dada la naturaleza de la interceptación, los atacantes han tenido la capacidad de llevar a cabo cualquier acción como si se realizara desde la cuenta autorizada, sin necesidad de conocer la contraseña de la cuenta»,* señaló el investigador.

> *«Esto implica que el atacante podría descargar la lista de contactos de la cuenta, acceder al historial de mensajes en el servidor sin cifrar, enviar mensajes nuevos o modificarlos en tiempo real».*

Se recomienda a los usuarios del servicio que consideren que sus comunicaciones de los últimos 90 días están comprometidas, además de *«verificar sus cuentas en busca de nuevas claves OMEMO y PGP no autorizadas en su almacenamiento PEP, y cambiar sus contraseñas».*

En un informe técnico propio, la empresa de ciberseguridad describe CVE-2023-46747 como

una vulnerabilidad de omisión de autenticación que podría llevar a una compromiso completo del sistema F5, permitiendo la ejecución de comandos arbitrarios con privilegios de administrador (root) en el sistema de destino. Esta vulnerabilidad se considera estrechamente relacionada con CVE-2022-26377.

Praetorian también recomienda que los usuarios limiten el acceso a la interfaz de usuario de gestión de tráfico (TMUI) desde Internet. Es importante destacar que CVE-2023-46747 es la tercera vulnerabilidad de ejecución remota de código no autenticada que se ha descubierto en TMUI, después de CVE-2020-5902 y CVE-2022-1388.

> *«Un error en la manipulación de solicitudes, que inicialmente parece tener un impacto bajo, puede convertirse en un problema grave cuando dos servicios diferentes transfieren la responsabilidad de autenticación entre sí. Enviar solicitudes al servicio 'backend' que asume que la autenticación es gestionada por el 'frontend' puede dar lugar a comportamientos inesperados»*, advierten los investigadores.