Cisco lanzó una nueva versión de su aplicación de mensajería y videoconferencia Jabber para Windows, que incluye parches para múltiples vulnerabilidad que de ser explotadas, podrían permitir que un atacante remoto autenticado ejecute código arbitrario.

Las vulnerabilidades, descubiertas por la compañía noruega de seguridad cibernética Watchcom durante un pentest, afectan a todas las versiones actualmente compatibles del cliente Jabber (12.1-12.9) y desde entonces han sido corregidas por la compañía.

Dos de los cuatro errores se pueden aprovechar para obtener la ejecución remota de código (RC) en los sistemas de destino mediante el envío de mensajes de chat especialmente diseñados en conversaciones grupales o individuos específicos.

El defecto más grave (CVE-2020-3495, con una puntuación CVSS 9.9), es causado por una validación incorrecta del contenido del mensaje, que podría ser aprovechado por un atacante enviando mensajes de Protocolo de presencia y mensajería extensible (XMPP) creados de forma malintencionada al software afectado.

> *«Un exploit exitoso podría permitir que el atacante haga que la aplicación ejecute programas arbitrarios en el sistema objetivo con los privilegios de la cuenta de usuario que ejecuta el software cliente Cisco Jabber, lo que posiblemente resulte en la ejecución de código arbitrario»*, dijo Cisco en un aviso.

Esto ocurre unos días después de que Cisco advirtiera sobre una vulnerabilidad de día cero explotada activamente en su software IOS XR.

XMPP (originalmente llamado Jabber), es un protocolo de comunicaciones basado en XML que se utiliza para facilitar la mensajería instantánea entre dos o más entidades de red.

También está diseñado para ser extensible con el fin de dar cabida a funciones adicionales, una de las cuales es XEP-0071: XHTML-IM, una especificación que establece las reglas para intercambiar contenido HTML mediante el protocolo XMPP.

La vulnerabilidad en Cisco Jabber surge de la vulnerabilidad de secuencias de comandos entre sitios (XSS) al analizar mensajes XHTML-IM.

> *«La aplicación no desinfecta adecuadamente los mensajes HTML entrantes y, en cambio, los pasa a través de un filtro XSS defectuoso»,* explicaron los investigadores de Watchcom.

Como consecuencia, un mensaje XMPP legítimo puede ser interceptado y modificado, haciendo que la aplicación ejecute un archivo ejecutable arbitrario existente dentro de la ruta del archivo local de la aplicación.

Para lograr esto, aprovecha una función vulnerable separada en Chromium Embedded Framework (CEF), un marco de código abierto que se utiliza para incrustar un navegador web Chromium dentro de otras aplicaciones, que podría ser abusado por un mal actor para ejecutar archivos .exe maliciosos en la máquina de la víctima.

Sin embargo, los atacantes deben tener acceso a los dominios XMPP de sus víctimas para enviar los mensajes XMPP maliciosos necesarios para aprovechar la vulnerabilidad con éxito.

Además, se podrían explotar otras tres vulnerabilidades en Jabber (CVE-2020-3430, CVE-2020-3498 y CVE-2020-3537) para inyectar comandos maliciosos y causar divulgación de información, incluida la posibilidad de recopilar de forma sigilosa los hash de contraseña NTLM de los usuarios.

Debido a que las aplicaciones de videoconferencia se están volviendo populares a raíz de la pandemia, es imperativo que los usuarios de Jabber actualicen a la última versión del software.

> *«Dada su nueva prevalencia en organizaciones de todos los tamaños, estas aplicaciones se están convirtiendo en un objetivo cada vez más atractivo para los*

> *atacantes. Mucha información sensible se comparte a través de videollamadas o mensajes instantáneos y las aplicaciones son utilizadas por la mayoría de los empleados, incluidos aquellos con acceso privilegiado a otros sistemas de TI»,* dijo Watchcom.