Cisco corrigió nuevamente más de cuatro vulnerabilidades críticas previamente reveladas en su aplicación de mensajería y videoconferencia Jabber, que fueron abordadas de forma inadecuada, dejando a sus usuarios susceptibles a ataques remotos.

Las vulnerabilidades, de ser explotadas exitosamente, podrían permitir que un atacante remoto autenticado ejecute código arbitrario en los sistemas de destino mediante el envío de mensajes de chat especialmente diseñados en conversaciones grupales o personas específicas.

Watchcom informó sobre las fallas al fabricante de equipos de red el 25 de septiembre, tres semanas después de que la compañía noruega de seguridad cibernética revelara públicamente múltiples deficiencias de seguridad en Jabber que se encontraron durante una prueba de penetración para un cliente en junio.

Las nuevas vulnerabilidades, que se descubrieron después de que uno de sus clientes solicitara una auditoría de verificación del parche, afectan a todas las versiones actualmente compatibles del cliente Cisco Jabber (12.1-12.9).

> *«Tres de las cuatro vulnerabilidades que Watchcom reveló en septiembre no han sido suficientemente mitigadas. Cisco lanzó un parche que solucionó los puntos de inyección que informamos, pero el problema subyacente no se ha solucionado. Como tal, pudimos encontrar nuevos puntos de inyección que podrían usarse para explotar las vulnerabilidades»,* dijo Watchcom en un informe.

La más crítica de las vulnerabilidades es CVE-2020-26085 (similar a CVE-2020-3945), que tiene una calificación de gravedad de 9.9 sobre 10, una vulnerabilidad de secuencia de comandos de sitios cruzados (XSS) sin clic que se puede usar para lograr ejecución remota de código escapando del recinto de seguridad CEF.

CEF Chromium Embedded Framework, es un marco de código abierto que se utiliza para incrustar un navegador web basado en Chromium dentro de otras aplicaciones.

Aunque el navegador integrado está protegido para evitar el acceso no autorizado a los archivos, los investigadores encontraron una forma de eludir las protecciones abusando de la función *window.CallCppFunction*, que está diseñada para abrir archivos enviados por otros usuarios de Cisco Jabber.

Todo lo que un adversario tiene que hacer es iniciar una transferencia de archivo que contenga un archivo .exe malicioso y obligar a la víctima a aceptarlo mediante un ataque XSS, luego activar una llamada a la función mencionada antes, haciendo que se ejecute el archivo en la máquina de la víctima.

Además, la vulnerabilidad no requiere interacción del usuario y se puede usar con gusanos, lo que significa que puede utilizarse para propagar automáticamente el malware a otros sistemas al disfrazar la carga útil en un mensaje de chat.

Una segunda vulnerabilidad, CVE-2020-27132, surge de la forma en que analiza las etiquetas HTML en los mensajes XMMPP, un protocolo de comunicaciones basado en XML que se utiliza para facilitar la mensajería instantánea entre dos o más entidades de red.

Debido a la falla de desinfección adecuada de estas etiquetas, un mensaje de transferencia de archivos inofensivo puede manipularse inyectando, por ejemplo, una etiqueta HTML de imagen que apunte a una URL maliciosa o incluso ejecutando código JavaScript malicioso.

> *«No se habían implementado medidas de seguridad adicionales y, por lo tanto, era posible obtener la ejecución remota de código y robar los hashes de contraseña NTLM utilizando este nuevo punto de inyección»,* dijeron los investigadores.

La tercera y última vulnerabilidad (CVE-2020-27127) es una falla de inyección de comandos relacionada con los controladores de protocolo, que se utilizan para informar al sistema operativo que abra URL específicas (por ejemplo, XMPP://, IM:7/ y TEL://) en Jabber, lo que hace posible que un atacante inserte indicadores de línea de comandos arbitrarios simplemente incluyendo un espacio en la URL.

Dada la naturaleza de autorreplicación de los ataques, se recomienda que los usuarios de Jabber actualicen a la última versión del software para mitigar el riesgo.

Watchom también recomienda que las organizaciones consideren deshabilitar la comunicación con entidades externas a través de Cisco Jabber hasta que todos los empleados hayan instalado la actualización.