Investigadores encontraron varias fallas de seguridad en las VPN corporativas populares que, según su informe, pueden utilizarse para romper silenciosamente las redes de la compañía y robar secretos comerciales.

Los investigadores de Devcore, Orange Tsai y Meh Chang, afirmaron que las fallas encontradas en los tres proveedores de VPN corporativos, Palo Alto Networks, Pulse Secure y Fortinet, son *«fáciles»* de explotar remotamente.

Estas VPN no son sus aplicaciones de VPN de consumidor tradicionales diseñadas para ocultar la identidad, pero son utilizadas por el personal que trabaja de forma remota para acceder a los recursos de la red de la empresa.

Normalmente, los empleados deben ingresar su nombre de usuario y contraseña corporativos, por lo general, usan códigos de dos factores. Al conectarse por medio de una conexión HTTPS (SSL), estos proveedores crean un túnel seguro entre la computadora del usuario y la red corporativa.

Pero Tsai y Chang aseguran que los errores que encontraron permitieron que cualquiera se infiltrara en secreto en la red de una empresa sin necesidad de un nombre de usuario o contraseña.

> *«Podríamos comprometer el servidor VPN y la intranet corporativa sin necesidad de autenticación, comprometer a todos los clientes de VPN y roban todos los secretos de las víctimas»,* dijo Tsai a TechCrunch en un correo electrónico.

> *«La SSL VPN es la forma más conveniente de conectarse a las redes corporativas. Por otro lado, para los piratas informáticos, SSL VPN debe estar expuesto a Internet, por lo que también es el camino más corto para comprometer su intranet»,* dijo Tsai.

En su primera reseña que detalla el error de Palo Alto Networks, los investigadores dijeron que una simple falla en el formato de la cadena, como el texto ingresado que el servidor no entiende correctamente, es suficiente para bloquear el servicio por completo. Varias compañías importantes utilizan la VPN GlobalProtect de Palo Alto, incluyendo Uber.

Los investigadores probaron el error en uno de los servidores internos de Uber en Palo Alto, según confirmaron. Uber rápidamente corrigió el error, pero dijo que su infraestructura interna era segura.

Los investigadores también utilizaron las vulnerabilidades para exponer fallas en los sistemas que pertenecen a Twitter, dijo Tsai.

> *«Obtuvimos el privilegio de root en el servidor VPN más importante de Twitter con éxito y obtuvimos la mayor severidad y la recompensa más alta de su programa de recompensas»*, agregó.

Cuando los investigadores se comunicaron en privado con Palo Alto sobre los errores, la compañía dijo que los errores ya se habían *«encontrado internamente»* y no emitieron una advertencia de seguridad pública.

El investigador de seguridad Kevin Beaumont, dijo en Twitter que parecía que el gigante de la seguridad emitió una «solución silenciosa» para este error *«realmente serio»* sin alertar a nadie.

Palo Alto finalmente emitió un aviso, un día después de que Tsai y Chang publicaran su informe en el blog detallando los errores.

Fortinet también publicó avisos para sus errores respectivos y actualizó el firmware para corregir dichas vulnerabilidades. Se recomienda a los administradores que actualicen sus puertas de enlace vulnerables a las últimas versiones.

El director de marketing de Pulse Secure, Scott Gordon, dijo que la compañía notificó a sus clientes sobre la vulnerabilidad y sobre un parche disponible a finales de abril. Gordon dijo que la compañía *«no tiene conocimiento»* de ningún exploit.

Palo Alto por su parte, reconoció que solucionó los errores pero no abordó las críticas de la comunidad de seguridad.

Un portavoz de Fortinet no quiso hacer comentarios antes de la publicación de los investigadores.

Seguridad Nacional advirtió a las empresas sobre una serie de vulnerabilidades en muchos de los principales proveedores de VPN corporativas, que también afectan a Palo Alto y Pulse Secure, así como a Cisco y F5 Networks.

Tsai y Chang están preparados para publicar los detalles de las fallas de Pulse Secure y Fortinet en los siguientes días.