Sophos informó que está solucionando una vulnerabilidad en sus dispositivos de firewall Cyberoam, que según un investigador de seguridad, puede permitir que un hacker obtenga acceso a la red interna de una empresa sin necesidad de una contraseña.

La vulnerabilidad permite a un atacante obtener de forma remota permisos de root en un dispositivo vulnerable, lo que le da el más alto nivel de acceso, mediante el envío de comandos maliciosos por medio de Internet. El ataque aprovecha el sistema operativo basado en la web que se encuentra en la parte superior del firewall de Cyberoam.

Los dispositivos de Cyberoam por lo general se utilizan en las grandes empresas, ubicados en el borde de una red y actúan como una puerta de entrada para permitir que los empleados entren mientras mantienen a los piratas informáticos fuera.

Estos dispositivos filtran el tráfico malo y evitan ataques de denegación de servicio y otros ataques basados en la red. También incluyen redes privadas virtuales (VPN), que permiten a los empleados remotos iniciar sesión en la red de su empresa cuando no se encuentran en la oficina.

Esta vulnerabilidad es muy similar a las fallas recientemente reveladas en los proveedores de VPN corporativos, particularmente de Palo Alto Networks, Pulse Secure y Fortinet, que permitieron a los piratas obtener acceso a la red corporativa sin necesidad de las credenciales de usuario.

Muchas de las grandes compañías tecnológicas, incluyendo a Uber o Twitter, se vieron afectadas por la tecnología vulnerable, lo que llevó a Seguridad Nacional a emitir un aviso para advertir acerca de los riesgos.

Mientras tanto, Sophos, que compró Cyberoam en 2014, emitió un breve aviso esta semana, diciendo que la compañía lanzó soluciones el pasado 30 de septiembre.

El investigador, que pidió permanecer en el anonimato, dijo que un atacante solo necesitaría una dirección IP de un dispositivo vulnerable. Dijo también que obtener dispositivos

vulnerables era algo fácil mediante el uso de motores de búsqueda como Shodan, que enumera alrededor de 96 mil dispositivos accesibles a Internet.

Un portavoz de Sophos cuestionó la cantidad de dispositivos afectados, pero no fue capaz de proporcionar una cifra más exacta.

> *«Sophos emitió una revisión automática para todas las versiones compatibles en septiembre, y sabemos que el 99% de los dispositivos ya se han parcheado automáticamente. Hay una pequeña cantidad de dispositivos que aún no se han parcheado porque el cliente ha desactivado la actualización automática y/o no son dispositivos con conexión a Internet»,* dijo el portavoz.

Los clientes aún afectados pueden actualizar sus dispositivos de forma manual, afirmó el vocero. Sophos agregó que la solución se incluirá en la próxima actualización de su sistema operativo CyberoamOS, pero no dijo cuándo se lanzará el software.

Adicionalmente, mencionó que esperan lanzar el código de prueba de concepto en los siguientes meses.