Cisco Systems acordó el pago de 8.6 millones de dólares para resolver una demanda que acusó a la compañía de vender un sistema de videovigilancia que contiene vulnerabilidades de seguridad severas a las agencias gubernamentales federales y estatales de Estados Unidos, aún sabiendo sobre ello.

Se cree que es el primer pago en un caso de *«Ley de Reclamaciones Falsas»* por incumplimiento de los estándares de seguridad cibernética.

La demanda comenzó hace ocho años, en 2011, cuando el subcontratista de Cisco se convirtió en denunciante, James Glenn, quien acusó a Cisco de seguir vendiendo una tecnología de videovigilancia a las agencias federales, aún luego de saber que el software era vulnerable a múltiples fallas de seguridad.

De acuerdo con los documentos judiciales compartidos por THN, Glenn y uno de sus colegas descubrieron múltiples vulnerabilidades en la suite Cisco Video Surveillance Manager (VSM) en septiembre de 2008, por lo que denunciaron el hecho a la compañía en octubre de 2008.

La suite VSM permite a los clientes administrar múltiples cámaras de video en distintas ubicaciones físicas por medio de un servidor centralizado, al que se puede acceder remotamente.

Según los informes, las vulnerabilidades podrían haber permitido que los hackers remotos obtuvieran acceso no autorizado al sistema de videovigilancia de forma permanente, lo que eventualmente les permitiría acceder a todas las fuentes de video, a todos los datos almacenados en el sistema, modificar o eliminar fuentes de video y eludir las medidas de seguridad.

Aparentemente, Net Design, el contratista de Cisco donde Glenn trabajaba en ese entonces, lo despidió poco después de informar acerca de las violaciones de seguridad de Cisco, que la compañía descubrió oficialmente como una medida de reducción de costos.

Sin embargo, en 2010, cuando Glenn se dio cuenta de que Cisco nunca solucionó dichos

problemas ni notificó a sus clientes, informó a la agencia federal de Estados Unidos, misma que luego lanzó una demanda argumentando que Cisco defraudó a los gobiernos federales, estatales y locales de Estados Unidos que compraron su producto.

Cisco vendió su suite VSM a departamentos de policía, escuelas, tribunales, oficinas municipales y aeropuertos, además de muchas otras agencias gubernamentales, incluyendo el Departamento de Seguridad Nacional de Estados Unidos, el Servicio Secreto, la Armada, el Ejército, la Fuerza Aérea, el Cuerpo de Marines y la Agencia Federal para el Manejo de Emergencias (FEMA).

> *«Cisco ha sabido de estas fallas críticas de seguridad por al menos dos años y medio, pero no ha notificado a las entidades gubernamentales que han comprado y siguen usando VSM acerca de la vulnerabilidad. Así, por ejemplo, un usuario no autorizado podría cerrar efectivamente un aeropuerto completo al tomar el control de todas las cámaras de seguridad y apagarlas. Alternativamente, el hacker podría acceder a los archivos de video de una gran entidad para ocultar o eliminar la evidencia de robo en video o espionaje»,* dice la demanda.

Después de la presentación de la demanda, la compañía reconoció las vulnerabilidades (CVE-2013-3429, CVE-2013-3430 y CVE-2013-3431), por lo que lanzó una versión actualizada de su software.

Como parte de la demanda, Cisco acordó el pago de 8.6 millones de dólares, de los cuales Glenn y sus abogados recibirán 1.6 millones y los 7 millones restantes serán para el gobierno federal y los 16 estados que compraron el producto afectado.

Cisco emitió una declaración oficial el miércoles como respuesta al último acuerdo, en la que dice que estaba *«complacido por haber resuelto»* la disputa de 2011 y que no *«hubo ninguna acusación o evidencia de que se produjo un acceso no autorizado al video de los clientes»* como resultado de la arquitectura de VSM.

Sin embargo, la compañía agregó que las transmisiones de video podrían *«teóricamente haber sido objeto de piratería»*, aunque la demanda no ha afirmado que nadie haya explotado las vulnerabilidades descubiertas por Glenn.