07/10/2025

Autoridades de EE.UU. emiten orden de ciberseguridad de “emergencia” tras el hackeo de al menos una agencia gubernamental

Las autoridades de ciberseguridad de Estados Unidos emitieron este jueves una “directiva de emergencia” que ordena a las agencias federales proteger sus redes ante un grupo avanzado de piratas informáticos que ha vulnerado al menos una agencia en una aparente campaña de espionaje.

Las autoridades no han precisado quién está detrás de los ataques, pero expertos independientes consideran que los responsables cuentan con respaldo estatal y operan desde China. Los atacantes han estado aprovechando fallas previamente desconocidas en programas de Cisco durante varios meses.

“Tenemos conocimiento de cientos de estos dispositivos [con el software afectado de Cisco] en el Gobierno federal”, dijo Chris Butera, alto funcionario de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés).

La directiva permitirá a las autoridades conocer “el alcance total de la vulneración en las agencias federales”, explicó Butera.

Unit 42, división de la firma de ciberseguridad Palo Alto Networks, dijo a CNN que considera que los piratas informáticos están en China. Sin embargo, otros grupos podrían intentar explotar las vulnerabilidades ahora que el problema es público y existe una actualización disponible.

“Como hemos visto antes, una vez que hay actualizaciones disponibles, es probable que los ataques aumenten a medida que los grupos delictivos descubran cómo aprovechar estas vulnerabilidades”, señaló Sam Rubin, vicepresidente senior de Unit 42.

La directiva ha generado una movilización en Washington para detectar a los piratas informáticos y desconectar cualquier dispositivo comprometido antes de que puedan causar más daños. Las agencias civiles tienen hasta el final del viernes para actualizar el software y reportar cualquier incidente.

Un portavoz de Cisco indicó que la empresa investigó los ataques en mayo junto con varias agencias gubernamentales y desde entonces ha identificado tres nuevas vulnerabilidades que los atacantes estaban explotando. La compañía instó a sus clientes a actualizar el software.

El Gobierno británico también alertó sobre la campaña de ataques, calificando el código malicioso utilizado como una “evolución significativa” respecto a herramientas anteriores.

La revelación se produce pocos días después de que investigadores de Mandiant, empresa propiedad de Google, informaran que otro grupo de presuntos piratas informáticos chinos había infiltrado a desarrolladores de software y despachos de abogados en Estados Unidos para recolectar información que beneficie a Beijing en su disputa comercial con Washington. Según Mandiant, la recuperación de esas vulnerabilidades podría tomar meses.

Fuente: https://cnnespanol.cnn.com/

LINK DE LA NOTICIA