BOLETÍN DE ALERTA

Boletín Nro.: 2015-1

Fecha de publicación: 23/02/2015

Tema: Adware pre-instalado en equipos Lenovo vulnerable a HTTPS Spoofing

Descripción:

Recientemente ha saltado a la luz que desde septiembre de 2014, Lenovo ha preinstalado un programa denominado "*Superfish VisualDiscovery*", un spyware/adware en algunos de sus computadoras con sistema operativo preinstalado (OEM). Superfish intercepta el tráfico de Internet del usuario de modo a proporcionar anuncios personalizados. Con el fin de interceptar las conexiones cifradas (los que usan HTTPS), el software instala un certificado raíz CA de confianza para Superfish. Todo el tráfico de navegación cifrado a Internet es interceptado, descifrado, y vuelto a cifrar por la aplicación para el navegador del usuario, lo que constituye un ataque clásico del tipo *Man In The Middle*. Como los certificados utilizados por Superfish son firmados por la CA (autoridad certificadora) instalada por el software, el navegador no mostrará ninguna advertencia de que el tráfico está siendo manipulado. Dado que la clave privada puede ser fácilmente obtenida desde el software Superfish, un atacante puede generar un certificado para cualquier sitio web que será confiable por un equipo que tenga el software Superfish instalado. Esto significa que sitios web, como bancas y el correo electrónico, pueden ser falsificadas sin que se despliegue una advertencia del navegador.

Aunque Lenovo ha declarado que han suspendido la pre-instalación de *Superfish VisualDiscovery*, los equipos que han traído el software ya instalado seguirán siendo vulnerable hasta que se adopten las medidas correctivas.

Superfish utiliza una librería de descifrado SSL de Komodia la cual es vulnerable, sin embargo dicha librería se encuentra presente también en otras aplicaciones, como por ejemplo KeepMyFamilySecure, Lavasoft, entre otras, por lo cual esta alerta no se limita a las aplicaciones y equipos mencionados. Cualquier aplicación que implemente las librerías de descifrado SSL de Komodia debería ser revisada.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Impacto:

Un equipo que tenga instalada la aplicación Superfish VisualDiscovery y/o cualquier aplicación que utilice las librerías de cifrado/descifrado SSL de Komodia podría ser vulnerable a ataques de SSL *spoofing* sin ninguna advertencia de los navegadores.

Sistemas afectados:

La lista de modelos de Lenovo afectados es la siguiente:

- Serie G: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45, G40-80
- Serie U: U330P, U430P, U330Touch, U430Touch, U530Touch
- Serie Y: Y430P, Y40-70, Y50-70, Y40-80, Y70-70
- Serie Z: Z40-75, Z50-75, Z40-70, Z50-70, Z70-80
- Serie S: S310, S410, S40-70, S415, S415Touch, S435, S20-30, S20-30Touch
- Serie Flex: Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 Pro, Flex 10
- Serie MIIX: MIIX2-8, MIIX2-10, MIIX2-11, MIIX 3 1030
- Serie YOGA: YOGA2Pro-13, YOGA2-13, YOGA2-11, YOGA3 Pro
- Serie E: E10-30

Otras aplicaciones que utilizan la librería de cifrado/descifrado SSL de Komodia:

- Atom Security, Inc
- Infoweise
- KeepMyFamilySecure
- Komodia
- Kurupira
- Lavasoft
- Qustodio
- Superfish
- Websecure Ltd

Detección:

Además de la lista de modelos de equipos y aplicaciones afectadas, podría haber más, por lo que se recomienda observar al tráfico de modo a buscar rastros. Para detectar un equipo que tenga Superfish VisualDiscovery instalado, se puede buscar una petición HTTP del tipo GET a superfish.aistcdn.com

La petición completa tendrá el siguiente formato:

http://superfish.aistcdn.com/set.php?ID=[GUID]&Action=[ACTION]

donde [ACTION] puede tomar los valores de 1 a 3.

Recomendaciones:

Los usuarios pueden desinstalar Superfish VisualDiscovery y/o otras aplicaciones que utilicen las librerías mencionadas. En el caso particular de los equipos Lenovo, se ha proveído una herramienta para la desinstalación de Superfish y la eliminación de todos sus certificados asociados, la cual puede ser obtenida en el siguiente enlace:

http://support.lenovo.com/us/en/product_security/superfish_uninstall

También es necesario eliminar todos los certificados raíz CA afectados, ya que la desinstalación de las aplicaciones no elimina los certificados.

Microsoft provee una guía específica para Windows:

1. Abrir el Administrador de Certificados haciendo click en el botón de **Start**, escribiendo **certmgr.msc** en el campo de búsqueda y ENTER. Aparecerá una ventana pidiendo la contraseña de Administrador o confirmación.
2. Ir a “Entidades de certificación raíz de confianza” > “Certificados”.
3. Seleccionar el certificado que se desea eliminar. En el caso de Superfish VisualDiscover, el certificado es emitido por “Superfish, Inc.”.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

4. Haga click derecho > Eliminar. Confirme que desea eliminar el certificado de forma permanente.

También se recomienda eliminar el certificado para los distintos exploradores y aplicaciones:

- Google Chrome: https://support.google.com/chrome/answer/95572?hl=es
- Mozilla Firefox y Thunderbird: https://wiki.mozilla.org/CA:UserCertDB#Deleting_a_Root_Certificate

En caso de que tenga conocimiento de otras aplicaciones que podrían estar utilizando las librerías mencionadas y/o de otros sistemas afectados, pueden contactarnos para investigar.

Información adicional:

- http://www.kb.cert.org/vuls/id/529496
- http://news.lenovo.com/article_display.cfm?article_id=1929
- https://technet.microsoft.com/en-us/library/cc772354.aspx
- http://windows.microsoft.com/en-us/windows-vista/view-or-manage-your-certificates

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py