Resumen de la solución

Protección frente a las vulnerabilidades de las aplicaciones móviles relacionadas con SSL

Hoy en día, en un momento en el que surgen continuamente nuevas aplicaciones móviles para los más variados fines y cuando cualquier idea innovadora para una app causa sensación, los usuarios no se plantean que sus aplicaciones pueden dejar su información confidencial desprotegida frente a ataques de intermediario (MITM) y, como resultado, poner en entredicho la confianza en su supuesta seguridad. Los desarrolladores de aplicaciones móviles también se toman a la ligera la privacidad y la seguridad de los usuarios. Sin embargo, ellos son los responsables de proteger la información privada de los usuarios frente a una lista de vulnerabilidades critpográficas, como BERserk y Heartbleed, entre otras, que no deja de crecer.

En septiembre de 2014, el equipo de respuesta ante emergencias informáticas (CERT) de la Carnegie Mellon University publicó una lista de apps para móviles que son vulnerables a los ataques MITM debido a que no validan correctamente los certificados SSL, dejando expuestos nombres de usuario y contraseñas ante los posibles agresores[1]. En enero de 2015 —cinco meses después—, McAfee® Labs observó que 18 de las 25 aplicaciones para móviles más descargadas de la lista seguían siendo vulnerables por validar incorrectamente la cadena digital, una de las vulnerabilidades más básicas relacionadas con SSL.

Visto que los desarrolladores de aplicaciones móviles no han respondido como corresponde a la creciente demanda de mayor privacidad y seguridad, es importante que tanto usuarios como empresas empleen todas las defensas a su alcance para aumentar al máximo la seguridad de las apps para móviles.

Defensas contra las vulnerabilidades de las aplicaciones móviles

A continuación proporcionamos algunas recomendaciones para protegerse del riesgo que implican las aplicaciones móviles vulnerables:

- Descargue e instale únicamente aplicaciones móviles conocidas, que hayan recibido comentarios positivos y procedentes de fuentes de confianza.
- Solo debe crear cuentas de inicio de sesión si comportan importantes ventajas frente a los usuarios "invitados". Emplee una contraseña diferente para cada cuenta.

intel Security

- Compruebe periódicamente las apps que se utilizan en el entorno empresarial para asegurarse de que no ponen en peligro la información confidencial a causa de alguna vulnerabilidad.
- Antes de descargarlas, consulte sus políticas de privacidad y averigüe a qué datos (ubicación y acceso a redes sociales) pueden acceder en los dispositivos de los usuarios y cómo los utilizan.

Cómo puede ayudarle Intel Security frente a las vulnerabilidades de las aplicaciones móviles

McAfee VirusScan® Mobile

McAfee VirusScan Mobile es un sistema antimalware que analiza y limpia los datos de los dispositivos móviles, evitando que se produzcan daños por virus, troyanos y otros programas maliciosos. McAfee VirusScan Mobile protege sus dispositivos móviles en los puntos de mayor exposición, como son los mensajes de correo electrónico entrantes y salientes, los mensajes de texto, los archivos adjuntos del correo electrónico y las descargas de Internet.

- **Detección de amenazas en tiempo real:** bloquea el malware del correo electrónico, los mensajes de texto y los archivos adjuntos sin que se produzcan demoras apreciables. McAfee VirusScan Mobile busca una amplia gama de amenazas maliciosas en menos de 200 milisegundos, lo que representa una protección automática y completa para los smartphones.
- **Privacidad de las aplicaciones:** averigua a qué información de identificación personal pueden acceder las aplicaciones instaladas para garantizar que los datos permanezcan seguros y que no corran riesgos innecesarios.
- **Reducción de la exposición a las vulnerabilidades relacionadas con SSL:** McAfee VirusScan Mobile emite notificaciones de alerta cuando las aplicaciones envían información confidencial a través de conexiones vulnerables, y clasifica las aplicaciones vulnerables como programas potencialmente no deseados (PUP).

Suites McAfee Complete Endpoint Protection

Las suites **McAfee Complete Endpoint Protection** se integran perfectamente en el reconocido software de administración **McAfee® ePolicy Orchestrator® (McAfee ePO™)**. Las suites McAfee Complete Endpoint Protection y el software McAfee ePO permiten a las empresas administrar y proteger a los usuarios de dispositivos móviles frente al malware para móviles, la exposición de los datos y otras amenazas.

- **Administración centralizada de antivirus y reputación de aplicaciones:** identifica automáticamente la reputación de las aplicaciones en cuanto a confianza y busca una gran cantidad de amenazas malintencionadas en menos de 200 milisegundos, lo que representa una protección automática y completa para los smartphones.
- **Un único panel:** proteja y administre los smartphones Google Android, Apple iOS y Microsoft Windows junto a los endpoints tradicionales en McAfee ePO, aprovechando sus funciones de automatización para desplegar e implementar las directivas sea cual sea el dispositivo o endpoint.
- **Implementación de directivas:** bloquee el acceso al correo electrónico corporativo si se detectan malware o PUP en las aplicaciones de los dispositivos de los usuarios. Aproveche la automatización de McAfee ePO para adoptar otras medidas en el dispositivo (por ejemplo, borrado de contenido, traslado a otra área del árbol del sistema donde se deniegue el acceso a la VPN corporativa, u otras acciones).

Intel Security True Key

True Key de Intel Security ofrece un modo fácil y seguro para iniciar una sesión en las apps desde un teléfono móvil. Con esta aplicación ya no es necesario recordar las contraseñas y los usuarios pueden acceder de forma inmediata a sus apps, sitios y dispositivos utilizando varias características que son exclusivas de cada uno de ellos.

- **Desbloqueo con dimensiones faciales:** permite iniciar una sesión utilizando rasgos exclusivos del usuario, como sus dimensiones faciales —la distancia entre los ojos y la nariz— o datos específicos, como los dispositivos que posee.
- **Creación y administración simplificadas de contraseñas únicas:** True Key recuerda las contraseñas y facilita a los usuarios acceso instantáneo a sitios web y apps para que no tengan que recordar varias contraseñas.
- **Identificación multifactor:** los usuarios pueden mejorar su perfil con varios factores de autenticación personales. Cuantas más características se añadan, más sólida será la protección.

Si protege a los empleados móviles frente a las aplicaciones mal implementadas evita riesgos innecesarios a la información confidencial de la empresa. La tecnología de seguridad de Intel Security permite a su empresa protegerse de forma proactiva frente a vulnerabilidades que ponen en jaque el modelo de confianza tradicional.

1. **http://www.kb.cert.org/vuls/id/582497**

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com