Boletín de Ciberseguridad | CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el martes 26 de junio del 2019

9VSA-00011-001 Vulnerabilidad de cross-site scripting (XSS) en Outlook para Android

Vulnerabilidad:

CVE-2019-1105

Resumen:

Microsoft ha publicado una actualización de seguridad para abordar la vulnerabilidad de cross-site scripting (XSS) en Outlook para Android, que permite a un atacante inyectar código JavaScript o similar aprovechando la forma en que Outlook analiza los mensajes de correo electrónico entrante.

Un atacante que explote con éxito esta vulnerabilidad podría realizar ataques de secuencias de comandos entre sitios en los sistemas afectados y ejecutar secuencias de comandos en el contexto de seguridad del usuario actual.

La actualización de seguridad corrige la forma en que Outlook para Android analiza los mensajes de correo electrónico especialmente diseñados para explotar esta vulnerabilidad.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/9VSA-00011-001.pdf

2CMV-00010-001 Explotación de la vulnerabilidad CVE-2017-8570 de Microsoft Office

Resumen:

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de correos electrónicos que pretenden engañar a las víctimas haciéndoles creer

que existe una reserva hotelera, poniendo como condición por parte del atacante para terminar la transacción, descargar documento adjunto en formato Word, denominado "detalle de la reserva.docx", el que se utiliza para explotar la vulnerabilidad CVE-2017-8570 de Office.

Vulnerabilidad:

CVE-2017-8570

Microsoft Office permite una vulnerabilidad de ejecución remota de código debido a la forma en la que gestiona los objetos en la memoria. Esto también se conoce como "Microsoft Office Remote Code Execution Vulnerability".

El parche está disponible en la siguiente URL de Microsoft:
https://portal.msrc.microsoft.com/enus/security-guidance/advisory/CVE-2017-8570

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/2CMV-00010-001.pdf

9VSA-00010-001 Vulnerabilidad en Apache Tomcat

Vulnerabilidad:

CVE-2019-10072

Resumen:

Apache ha publicado un aviso de seguridad para abordar la vulnerabilidad en Apache Tomcat, que permite a un atacante realizar de forma remota una denegación de servicio.
Mediante esta actualización se corrige una solución incompleta para el agotamiento de la ventana de conexión HTTP/2 durante la escritura. Al no enviar mensajes WINDOW_UPDATE para la ventana de conexión (stream 0), los clientes podrían hacer que los hilos del lado del servidor se bloquearan, provocando una denegación de servicio.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/9VSA-00010-001.pdf

8FPH-00038-001 Campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado

Resumen:
El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco para que vuelvan a registrar su cuenta, de lo contraria podría quedar bloqueada. Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

> *"Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño."*

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00038-001.pdf

8FPH-00037-001 Campaña de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Internos.

Resumen:

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Internos. Los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de un "aviso (SII)" o "segundo aviso (SII)". El contenido del mensaje advierte a los usuarios que, para evitar una sanción económica, que podría ascender a 75 UTM, deben descargar un supuesto documento de restitución de la declaración. Al seleccionar dicho enlace, se desencadena la descarga de archivos maliciosos, que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando, además, puertas traseras con la posibilidad de infectar con otros malware según sea el propósito del atacante.

> *"Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus*

potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.“

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00037-001.pdf

8FPH-00036-001 Detección de 41 dominios de suplantación del Banco Chile que intentan engañar a los clientes

Resumen:
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 41 dominios de suplantación del Banco Chile que intentan engañar a los clientes, utilizando técnicas de phishing.

Los delincuentes intentan convencer a sus víctimas a través de correos electrónicos u otros medios para que accedan a los sitios aquí indicados, con la finalidad de que los clientes entreguen sus credenciales de acceso a sus cuentas bancarias.

“Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.“

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00036-001.pdf

8FPH-00035-001 Campaña de Phishing a través de un correo electrónico que supuestamente proviene de la empresa de streaming Netflix

Resumen:

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que supuestamente proviene de la empresa de streaming Netflix. Dicho correo busca engañar al usuario indicándole que debe actualizar el detalle de pago dentro de las próximas 24 horas para evitar interrupción de sus servicios. Con esta premisa se intenta inducir al usuario a seleccionar el link que aparece en el correo, direccionándolo a un sitio web falso.

"Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño."

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00035-001.pdf

8FPH-00034-001 Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Scotibank

Resumen:

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Scotibank. El correo trata de persuadir al cliente que tiene que aprobar un abono, ya que fue premiado por un aumento de su línea de crédito de $ 999.999 y además participará de un sorteo de 60 televisores Led Samsung de 55 pulgadas, 100 Play Station 4 y 250 celulares Motorola E5 16GB. Este correo además intenta engañar al usuario, mostrando que su origen es del dominio "meteochile.cl" perteneciente a la Dirección Meteorólogica de Chile, siendo que, en realidad, el correo no proviene de dicho dominio.

"Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño."

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00034-001.pdf

8FPH-00033-001 Campaña de phishing basada en una supuesta funcionalidad reducida de su correo

Resumen:

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing, a través de un correo electrónico que intenta engañar al usuario

para que ingrese sus credenciales de correo, mencionando que debe actualizar sus datos para evitar una funcionalidad reducida. Este correo proviene de la cuenta jguillen@proviasdes.gob.pe.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00033-001.pdf

8FPH-00032-001 Phishing con Malware en Correo que Suplanta a Empresa de Streaming

Resumen:

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene de la empresa de streaming Netflix, Los delincuentes buscan engañar a los usuarios insinuando que su cuenta presenta información incorrecta debiendo actualizarla antes de 48 horas, de lo contrario se procederá a la suspensión del servicio. Los delincuentes buscan persuadir a sus víctimas para que seleccionen el link que aparece en el correo, lo que los direccionará a un sitio falso.

"Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma, el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño."

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00032-001.pdf