13BCS-00022-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática
Publicado el Jueves 12 de Septiembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 05 y el miércoles 11 de Septiembre.

Noticias

Publicado 06 septiembre, 2019

Hackers demandan $ 5,3 millones de dólares después de bloquear las computadoras de la ciudad New Bedford, Massachusetts, utilizando el RYUK Ransomware

El ransomware originalmente apareció en agosto de 2018 y se distribuyó a través de campañas masivas de spam y kits de explotación, además de operaciones específicas, tales como mapeo de redes extensas, piratería y recopilación de credenciales necesarias antes de cada operación. Hace unos meses atrás, el National Cyber Security Center del Reino Unido emitió una alerta global sobre el ransomware Ryuk. El CSIRT del Gobierno de Chile también replicó la alerta a nivel local.

Enlace:
https://www.csirt.gob.cl/noticias/hackers-demandan-53-millones-de-dolares-despues-de-bloquear-las-computadoras-de-la-ciudad-new-bedford-massachusetts-utilizando-el-ryuk-ransomware/

Publicado 09 septiembre, 2019

Expertos de seguridad de Google removieron 24 aplicaciones desde Google Play porque estaban infectadas por “The Joker” spyware

La aplicación carga un archivo ejecutable Dalvik de segunda etapa (DEX), que es un archivo de código para el sistema operativo Android. El archivo, a su vez, elimina la carga útil, que incluye capacidades para capturar mensajes SMS, listas de contactos e información del dispositivo desde el teléfono de la víctima.

Enlace:
https://www.csirt.gob.cl/noticias/expertos-de-seguridad-de-google-removieron-24-aplicaciones-desde-google-play-porque-estaban-infectadas-por-the-joker-spyware/

8FFR-00045-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRADULENTO

Alerta de seguridad informática	8FFR-00045-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2019
Última revisión	07 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoestado.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00045-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00045-001/

8FFR-00046-001 CSIRT ADVIERTE SOBRE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00046-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2019
Última revisión	07 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoEstado.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00046-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00046-001/

8FFR-00047-001 CSIRT DA CUENTA DE NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00047-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2019
Última revisión	07 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoestado.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00047-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00047-001/

8FFR-00048-001 CSIRT ADVIERTE DE WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR-00048-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancobci.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00048-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00048-001/

8FFR-00049-001 CSIRT INFORMA DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00049-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2019
Última revisión	07 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoEstado.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00049-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00049-001/

8FFR-00050-001 CSIRT INFORMA SOBRE NUEVO SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00050-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Septiembre de 2019
Última revisión	07 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoEstado.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00050-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00050-001/

8FFR-00051-001 CSIRT INFORMA DE SITIO FRAUDULENTO QUE SUPLANTA A UNA WEB BANCARIA

Alerta de seguridad informática	8FFR-00051-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancoChile.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00051-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00051-001/

8FFR-00052-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO QUE SUPLANTA A PORTAL BANCARIO

Alerta de seguridad informática	8FFR-00052-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del banco ScotiaBank.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00052-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00052-001/

8FFR-00053-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO BANCARIO

Alerta de seguridad informática	8FFR-00053-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del banco ScotiaBank.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00053-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00053-001/

8FFR-00054-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO QUE SUPLANTA A PORTAL BANCARIO

Alerta de seguridad informática	8FFR-00054-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial del banco ScotiaBank.cl, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/09/8FFR-00054-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00054-001/

8FPH-00059-001 CSIRT ADVIERTE DE PHISHING ASOCIADO A UN AUMENTO DE CUPO EN LÍNEA Y TRARJETA DE CRÉDITO

Alerta de seguridad informática	8FPH-00059-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico dirigido a los usuarios del Banco de Chile. El mensaje del correo hace referencia a un eventual aumento de cupo en la línea de crédito y/o tarjeta de crédito, cuya vigencia es solo por el mes de Septiembre. A través de ingeniería social, los criminales intentan persuadir a los usuarios para ingresar al hipervínculo asociado a la oferta. Si las personas ingresan al enlace, se exponen a que el atacante robe sus credenciales desde un sitio que imita al original del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/09/8FPH-00059-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00059-001/

8FPH-00060-001 CSIRT ADVIERTE DE PHISHING EN PROCEDIMIENTO PARA SINCRONIZAR DIGIPASS

Alerta de seguridad informática	8FPH-00060-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico dirigido a los usuarios del Banco de Chile. El mensaje del correo intenta persuadir a los usuarios de ingresar a un hipervínculo como parte del procedimiento para sincronizar su digipass. A través del uso de técnicas de ingeniería social, los criminales tratan de engañar a las personas enfatizando la urgencia de realizar este trámite a través de la banca de internet en un plazo máximo de 48 horas tras la recepción del correo, de lo contrario su cuenta sería inhabilitada y obligaría a la persona a realizar el trámite directamente en la sucursal más cercana para solicitar una nueva tarjeta. Si la persona llega a ingresar al hipervínculo señalado, se expone a que el atacante robe sus credenciales desde un sitio semejante al original del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/09/8FPH-00060-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00060-001/

8FPH-00061-001 CSIRT ADVIERTE DE PHISHING POR ACTUALIZACIÓN DE CUENTA

Alerta de seguridad informática	8FPH-00061-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Septiembre de 2019
Última revisión	10 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta persuadir a los usuarios del Banco Estado para que realicen una actualización utilizando un enlace dentro del cuerpo del correo. El mensaje señala que se realizó una actualización de las cuentas, pero que ya estarían operativos. Producto de la actualización, los criminales advierten a la potencial víctima sobre la detección de un error en su cuenta, razón por la que se procedió al bloqueo de la misma de forma temporal. Los estafadores señalan que la única forma de desbloquear la cuenta es ingresando al enlace malicioso oculto en el enlace. A través de ingeniería social, el atacante incita a sus víctimas para ingresar al enlace, exponiéndolos al robo de sus credenciales desde un sitio semejando al del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/09/8FPH-00061-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00061-001/

Alertas de Malware

2CMV-00031-001 CSIRT ADVIERTE DE MALWARE DIRIGIDO CONTRA LA CIUDADANÍA Y SISTEMA BANCARIO VÍA USO PROXY CHANGE Y EXTENSIÓN DE CHROME

Alerta de seguridad informática	2CMV-00031-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Septiembre de 2019
Última revisión	05 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha detectado un nuevo script malicioso que se encuentra activo. El malware tiene relación con el Informe sobre actividad maliciosa dirigida contra la ciudadanía y el sistema financiero nacional vía uso proxy change y extensión de Chrome publicado por el CSIRT de Gobierno recientemente. (La información está disponible en el sitio http://www.csirt.gob.cl en la sección reportes. El documento identificado como 10CND-00017-001 fue publicado el 4 de septiembre de 2019).

Este malware realiza dos acciones maliciosas. La primera, a través de una extensión de Google Chrome que al ser instalada redirige a los usuarios a sitios bancarios fraudulentos. La segunda acción realiza una configuración en las opciones de proxy del sistema operativo para los mismos fines.
Los usuarios se exponen a ser víctimas del robo de sus credenciales bancarias por la navegación en un sitio bancario fraudulento.
En el informe indicado anteriormente fueron identificados 1.121 hosts infectados. Con los nuevos hallazgos que se han realizado fueron identificados otros 373 host. Este nuevo script tiene el mismo modus operandi pero se diferencia por la complejidad en la técnica de ofuscación.

Enlace

https://www.csirt.gob.cl/media/2019/09/2CMV-00031-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00031-001/

Informes

2CMV-00031-001 CSIRT ADVIERTE DE MALWARE DIRIGIDO CONTRA LA CIUDADANÍA Y SISTEMA BANCARIO VÍA USO PROXY CHANGE Y EXTENSIÓN DE CHROME

Alerta de seguridad informática	10CND-00017-001
Clase de alerta	Código Malicioso
Tipo de incidente	Informe de Seguridad - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó una actividad maliciosa en un script que se encuentra activo en el repositorio de Pastebin. Su análisis permitió identificar que el script está dirigido contra la ciudadanía y el sistema financiero nacional.
Se encontraron dos acciones maliciosas. La primera, a través de una extensión de Google Chrome que al ser instalada redirige a los usuarios a sitios fraudulentos. La segunda acción realiza una configuración en las opciones de proxy del sistema operativo para los mismos fines.
El principal riesgo es que podrían ser robados una gran cantidad de datos bancarios en la medida que persista su actividad.

Enlace

https://www.csirt.gob.cl/media/2019/09/10CND-00017-001.pdf
https://www.csirt.gob.cl/reportes/10cnd-00017-001/

14IMT-00013-001 INFORME DE GESTIÓN DE CSIRT MES DE AGOSTO

Resumen

El informe contiene un resumen de la totalidad de los tickets procesados en el mes de agosto de 2019. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets.

El informe también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso del mes de agosto y también muestra la proporción de aquellos que quedan por terminar.

Asimismo, en este documento se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.

Este reporte mensual muestra, además, el origen o procedencia de la información que procesa CSIRT –si es interna o externa- y presenta en términos porcentuales el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

Adicionalmente, también se entrega un desagregado con el detalle que permite conocer la participación –en cantidades y en términos porcentuales- de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.

Finalmente, se presenta información proveniente de la plataforma MISP que contiene la cantidad de posibles IoCs o –Índices de Compromiso- que se hayan detectado. Esta información es relevante para CSIRT dado que se utiliza como punto de partida para validar correlaciones con todas nuestras plataformas de análisis. En el informe se expone una tabla donde se puede enumerar la cantidad de IoCs detectados en el presente mes, los cuales se presentan diferenciados en base a direcciones IP o a URL.

Enlace

El informe está disponible en el siguiente enlace:
https://www.csirt.gob.cl/estadisticas/informe-de-gestion-de-csirt-mes-de-agosto/
https://www.csirt.gob.cl/media/2019/09/14IMT-00013-001.pdf

Vulnerabilidades

9VSA-00044-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIONES EN FIREFOX

Alerta de seguridad informática	9VSA-00044-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de septiembre de 2019
Última revisión	05 de septiembre de 2019

Vulnerabilidad

CVE-2019-11751	CVE-2019-11752
CVE-2019-11746	CVE-2019-9812
CVE-2019-11744	CVE-2019-11741
CVE-2019-11742	CVE-2019-11743
CVE-2019-11736	CVE-2019-11748
CVE-2019-11753	CVE-2019-11749

CVE-2019-5849
CVE-2019-11750
CVE-2019-11737
CVE-2019-11738
CVE-2019-11747
CVE-2019-11734
CVE-2019-11735
CVE-2019-11740

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por MOZILLA referente a vulnerabilidades detectadas en Firefox, explorador para navegación en internet, junto a su respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00044-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00044-001/

9VSA-00045-001 CSIRT COMPARTE ACTUALIZACIONES EN CISCO

Alerta de seguridad informática	9VSA-00045-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de septiembre de 2019
Última revisión	06 de septiembre de 2019

Vulnerabilidades

CVE-2019-12632
CVE-2019-12644
CVE-2019-12645
CVE-2019-12635
CVE-2019-12633
CVE-2019-1976
CVE-2019-1939

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por CISCO referente a vulnerabilidades detectadas en varios de sus productos y sus respectivos parches.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00045-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00045-001/

9VSA-00008-002 CSIRT REITERA ALERTA SOBRE VULNERABILIDAD CONOCIDA COMO BLUEKEEP

Alerta de seguridad informática	9VSA-00008-002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Junio de 2019
Última revisión	07 de Septiembre de 2019

Vulnerabilidad

CVE-2019-0708

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, reitera la alerta informada en junio pasado y advertida originalmente por la Agencia CISA del Departamento de Seguridad Interior de los Estados Unidos, para proporcionar información sobre la vulnerabilidad conocida como «BlueKeep», que existe en Sistemas Operativos de Microsoft Windows (OS), incluidas las versiones de 32 y 64 bits, así como todas las versiones del Service Pack. Un atacante puede aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00008-002.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00008-002/

9VSA-00046-001 CSIRT COMPARTE VULNERABILIDAD POR EL HALLAZGO DEL EXPLOIT DEJABLUE

Alerta de seguridad informática	9VSA-00046-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Septiembre de 2019
Última revisión	09 de Septiembre de 2019

Vulnerabilidad

CVE-2019-1181
CVE-2019-1182

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a vulnerabilidades detectadas que pueden comprometer la seguridad en sus sistemas operativos. Si bien los CVE's ya fueron advertidos a la comunidad en informes pasados, debido al hallazgo de un nuevo exploit llamado DejaBlue, y por su parecido con BlueKeep (otra falla de seguridad de RDP expuesta en mayo), el CSIRT de Gobierno ha estimado necesario publicar esta alerta de seguridad.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00046-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00046-001/

9VSA-00047-001 CSIRT COMPARTE ACTUALIZACIONES PARA LAS VULNERABILIDADES DE PHP

Alerta de seguridad informática	9VSA-00047-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Septiembre de 2019
Última revisión	10 de Septiembre de 2019

Vulnerabilidad

CVE-2019-11041
CVE-2019-11042

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por PHP referente a vulnerabilidades detectadas en su producto y los respectivos parches. Este resumen incluye los CVE's involucrados, una descripción del impacto de los productos afectados y medidas de mitigación.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00047-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00047-001/

9VSA-00048-001 CSIRT COMPARTE ACTUALIZACIONES DE MICROSOFT, PARCHES CRÍTICOS PARA RCE Y PARA RDP CLIENTE

Alerta de seguridad informática	9VSA-00048-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Septiembre de 2019
Última revisión	11 de Septiembre de 2019

Vulnerabilidad

CVE-2019-1142	CVE-2019-1247	CVE-2019-1263
CVE-2019-1209	CVE-2019-1248	CVE-2019-1264
CVE-2019-1216	CVE-2019-1249	CVE-2019-1265
CVE-2019-1219	CVE-2019-1250	CVE-2019-1274
CVE-2019-1231	CVE-2019-1251	CVE-2019-1282
CVE-2019-1240	CVE-2019-1252	CVE-2019-1283
CVE-2019-1241	CVE-2019-1254	CVE-2019-1286
CVE-2019-1242	CVE-2019-1257	CVE-2019-1293
CVE-2019-1243	CVE-2019-1259	CVE-2019-1295
CVE-2019-1244	CVE-2019-1260	CVE-2019-1296
CVE-2019-1245	CVE-2019-1261	CVE-2019-1297
CVE-2019-1246	CVE-2019-1262	CVE-2019-1299
CVE-2019-0928	CVE-2019-1253	CVE-2019-1284
CVE-2019-1138	CVE-2019-1256	CVE-2019-1285
CVE-2019-1208	CVE-2019-1266	CVE-2019-1287
CVE-2019-1214	CVE-2019-1267	CVE-2019-1289
CVE-2019-1215	CVE-2019-1268	CVE-2019-1292
CVE-2019-1217	CVE-2019-1269	CVE-2019-1294
CVE-2019-1220	CVE-2019-1270	CVE-2019-1298
CVE-2019-1221	CVE-2019-1271	CVE-2019-1300
CVE-2019-1232	CVE-2019-1272	CVE-2019-1301
CVE-2019-1233	CVE-2019-1273	CVE-2019-1302
CVE-2019-1235	CVE-2019-1277	CVE-2019-1303
CVE-2019-1236	CVE-2019-1278	CVE-2019-1305
CVE-2019-1237	CVE-2019-1280	CVE-2019-1306
CVE-2019-0787	CVE-2019-0788	CVE-2019-1290

CVE-2019-1291

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a septiembre del 2019, parchando un total de 79 vulnerabilidades en sus softwares. Del total anterior, 17 han sido clasificados como críticos, 61 como importantes y uno como moderado.

Además se recalca que 4 de los parches críticos hacen referencia a vulnerabilidades de ejecución remota arbitraria de código o RCE (por sus siglas en inglés) para la aplicación integrada de cliente de escritorio remoto de Windows, lo que podría permitir que un servidor RDP malicioso comprometa el equipo del cliente.

A diferencia del error de BlueKeep, las vulnerabilidades RDP recién parcheadas son todas del lado del cliente, lo que requiere que un atacante engañe a las víctimas para que se conecten a un servidor RDP malicioso a través de ingeniería social, envenenamiento de DNS o utilizando una técnica Man in the Middle (MITM).

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00048-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00048-001/

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad:

IP's	Causa Asociada
143.215.247.67	Port Scan
208.73.210.217	Hacking
42.231.162.209	Hacking
138.68.212.142	Port Scan
5.9.157.50	Malware
42.231.162.194	Hacking
159.203.203.52	Port Scan
222.186.19.221	Port Scan
187.17.111.47	Phishing
181.170.121.9	Malware
118.25.2.59	Malware
119.28.134.196	Malware
115.159.100.50	Malware
123.207.107.218	Malware
182.61.106.24	Malware

203.195.189.185	Malware
213.222.56.130	Malware
124.205.212.31	Malware
132.232.212.9	Malware
110.170.148.135	Malware
113.53.231.2	Malware
118.25.105.88	Malware
119.28.134.196	Malware
195.154.86.34	Malware
203.195.218.37	Malware
213.222.56.130	Malware
46.246.42.134	Malware
60.29.69.30	Malware
185.216.140.93	Malware
148.70.211.244	Malware
148.70.226.133	Malware
150.109.197.35	Malware
101.204.227.166	Malware
101.231.101.134	Malware
103.124.144.146	Malware
103.194.105.146	Malware
103.208.35.211	Malware
103.240.182.140	Malware
103.68.224.1	Malware
103.78.103.58	Malware
103.86.67.42	Malware
104.128.230.115	Malware
192.162.101.249	Malware
202.79.165.140	Malware
190.81.169.18	Malware
176.121.14.184	Malware
106.12.187.83	Malware
106.13.21.110	Malware
106.13.44.34	Malware
106.13.46.149	Malware
106.13.48.54	Malware
106.75.129.166	Malware
109.74.15.197	Malware
110.170.148.135	Malware
111.161.41.86	Malware
111.230.23.22	Malware
111.231.141.38	Malware

111.231.204.34	Malware
111.231.205.63	Malware
111.231.93.210	Malware
112.213.103.115	Malware
112.213.105.101	Malware
112.213.106.177	Malware
112.90.56.226	Malware
114.118.7.89	Malware
114.242.85.229	Malware
115.159.100.50	Malware
115.159.107.118	Malware
115.159.108.113	Malware
115.159.198.81	Malware
115.159.206.134	Malware
116.196.101.146	Malware
116.204.168.19	Malware
116.255.183.105	Malware
118.24.171.154	Malware
118.24.38.122	Malware
218.156.38.233	Malware
202.79.174.122	Malware
114.34.144.97	Malware
92.53.65.164	Malware
148.70.211.244	Malware
148.70.226.133	Malware
150.109.197.35	Malware
150.109.61.170	Malware
150.109.67.14	Malware
152.32.128.223	Malware
154.8.200.196	Malware
159.192.96.176	Malware
167.71.192.113	Malware
168.128.148.202	Malware
118.24.4.204	Malware
118.24.68.65	Malware
118.24.72.48	Malware
118.25.108.250	Malware
118.25.111.12	Malware
118.25.192.84	Malware
118.25.71.229	Malware
118.89.57.149	Malware
119.196.130.106	Malware

119.27.175.41	Malware
171.100.119.102	Malware
175.102.10.147	Malware
180.215.80.2	Malware
182.140.235.190	Malware
182.61.186.210	Malware
183.131.65.72	Malware
185.170.210.65	Malware
186.201.194.58	Malware
188.131.144.65	Malware
190.216.102.67	Malware
190.5.135.121	Malware
192.169.231.213	Malware
193.112.185.115	Malware
193.112.212.143	Malware
193.169.254.11	Malware
195.154.86.34	Malware
197.159.135.49	Malware
201.149.82.181	Malware
201.76.163.138	Malware
202.39.64.122	Malware
119.28.134.196	Malware
119.28.193.18	Malware
119.29.161.237	Malware
119.29.232.38	Malware
119.29.9.42	Malware
119.3.233.30	Malware
119.3.93.53	Malware
120.39.243.43	Malware
121.201.46.229	Malware
121.9.250.17	Malware
202.53.137.92	Malware
202.53.139.15	Malware
202.62.11.76	Malware
202.79.167.62	Malware
203.157.219.17	Malware
203.189.235.138	Malware
203.195.238.41	Malware
203.195.254.67	Malware
203.43.88.79	Malware
210.209.87.134	Malware
211.147.238.121	Malware

122.112.230.32	Malware
122.142.17.11	Malware
122.152.198.125	Malware
122.154.230.146	Malware
122.155.204.198	Malware
123.206.128.145	Malware
123.207.107.218	Malware
123.207.52.78	Malware
124.156.200.56	Malware
202.53.137.92	Malware
202.53.139.15	Malware
202.62.11.76	Malware
202.79.167.62	Malware
203.157.219.17	Malware
203.189.235.138	Malware
203.195.238.41	Malware
203.195.254.67	Malware
203.43.88.79	Malware
210.209.87.134	Malware
211.147.238.121	Malware
124.156.240.114	Malware
124.158.175.50	Malware
125.136.150.146	Malware
129.204.112.220	Malware
129.204.161.136	Malware
129.204.201.32	Malware
129.204.40.54	Malware
129.204.51.140	Malware
129.211.128.221	Malware
129.211.87.192	Malware
129.28.151.40	Malware
132.232.107.172	Malware
132.232.168.65	Malware
132.232.200.165	Malware
132.232.249.220	Malware
132.232.32.13	Malware
132.232.88.174	Malware
134.175.102.205	Malware
134.175.157.215	Malware
139.159.154.70	Malware
221.179.172.85	Malware
222.186.169.155	Malware

222.186.43.73	Malware
222.189.228.155	Malware
223.221.240.218	Malware
36.66.150.227	Malware
36.66.171.205	Malware
36.7.69.254	Malware
36.89.80.186	Malware
40.123.44.133	Malware
139.199.119.67	Malware
139.199.131.245	Malware
139.199.184.166	Malware
139.199.96.44	Malware
139.9.7.31	Malware
140.143.167.250	Malware
140.143.47.55	Malware
140.143.71.1	Malware
148.70.125.239	Malware
42.51.33.118	Malware
45.40.246.110	Malware
46.246.42.134	Malware
46.246.45.175	Malware
49.234.101.112	Malware
49.234.101.15	Malware
49.249.249.202	Malware
5.166.47.194	Malware
5.196.162.100	Malware
51.15.25.175	Malware
51.159.7.51	Malware
51.79.43.14	Malware
54.37.230.33	Malware
54.39.98.171	Malware
58.242.233.108	Malware
58.87.77.250	Malware
60.21.253.82	Malware
60.251.46.85	Malware
60.29.69.30	Malware
61.19.27.157	Malware
62.165.50.254	Malware
62.234.108.128	Malware
62.4.27.96	Malware
80.82.78.57	Malware
81.2.255.24	Malware

81.22.100.7	Malware
89.232.204.93	Malware
93.61.124.33	Malware
94.102.50.96	Malware
94.177.228.193	Malware
94.177.231.9	Malware
94.191.28.13	Malware
94.191.77.57	Malware
94.191.84.62	Malware
94.191.92.102	Malware
94.191.99.107	Malware
94.255.177.203	Malware
193.148.69.229	Port Scan
124.108.21.10	Port Scan
46.182.111.74	Port Scan
182.147.243.50	Port Scan
185.148.39.43	Port Scan
14.192.7.2	Port Scan
23.254.224.243	Port Scan
138.68.223.70	Port Scan
136.68.208.185	Port Scan
185.175.93.105	Port Scan
185.175.93.101	Port Scan
89.248.172.85	Port Scan
89.248.168.202	Port Scan
193.148.69.229	Port Scan
157.245.77.163	Malware
206.189.155.31	Malware
157.245.76.212	Malware

URL	Motivo
https[://]personasweb.email/Portalsite/bancochile/wps/wcm/connect/Personas/Portal/public/cliente	Phishing
http://www[.]accept-support[.]xyz	Malware
tp[://]bancoestado-cl-imagenes-comun2008[.]zonaviabcpe[.]com	Phishing
http[://]poseristas[.]gr/wp/wp-includes/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-per	Phishing
http://spart4.com/abc4/imagenes/comun2008/banca-en-linea-personas.html	Phishing
http://3.122.143.26/	Malware
http://joker2.dolphinsclean.com/	Malware
http://beatleslover.com/	Malware
http://47.254.144.154/	Malware

https://s3.amazonaws.com/	Malware
https://aliyuncs.com/	Malware
http://wwwbancafalabellas-pe.com/TechBank/sso/	Phishing
https[://]oferta-avance-de-tarjeta[.]gq/www[.]bancoedwards[.]cl/Login[.]html	Phishing
http://www.scotiaaweb.xyz/	Phishing
http[:]//gothamglassworks[.]com/dr9/imagenes/comun2008/banca-en-linea-personas.html	Phishing
http[:]//axnpop[.]site/readme/Simuladores/	Phishing

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.12 09:23:36 -03'00'