CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 31 de Enero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 23 de y el miércoles 29 de Enero de 2020.

Falsificación de Registro o Identidad

8FFR20-00188-01 CSIRT ADVIERTE DE WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR20-00188-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero de 2020

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 de Banco Scotiabank, 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://csirt.gob.cl/alertas/8ffr20-00188-01/

https://csirt.gob.cl/media/2020/01/8FFR20-00188-01.pdf

8FFR20-00189-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00189-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero de 2020

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 de Banco BCI, 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://csirt.gob.cl/alertas/8ffr20-00189-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00189-01.pdf

8FFR20-00190-01 CSIRT ADVIERTE DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR20-00190-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero de 2020

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 de Banco de Chile, 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://csirt.gob.cl/alertas/8ffr20-00190-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00190-01.pdf

8FFR20-00191-01 CSIRT ADVIERTE DE SITIO BANCARIOS FRAUDULENTO

Alerta de seguridad informática	8FFR20-00191-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero de 2020

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 de Banco Estado, 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://csirt.gob.cl/alertas/8ffr20-00191-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00191-01.pdf

8FFR20-00192-01 CSIRT ADVIERTE DE SITIO BANCARIOS FRAUDULENTO

Alerta de seguridad informática	8FFR20-00192-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Enero de 2020
Última revisión	26 de Enero de 2020

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 de Banco Falabella, 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://csirt.gob.cl/alertas/8ffr20-00192-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00192-01.pdf

8FFR20-00193-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00193-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Enero de 2020
Última revisión	26 de Enero de 2020

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 de Banco de Chile, 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://csirt.gob.cl/alertas/8ffr20-00193-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00193-01.pdf

8FFR20-00194-01 CSIRT ADVIERTE SOBRE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00194-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Enero de 2020
Última revisión	26 de Enero de 2020

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 de Banco Scotiabank, 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://csirt.gob.cl/alertas/8ffr20-00194-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00194-01.pdf

8FFR20-00195-01 CSIRT ADVIERTE DE 4 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00195-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Enero de 2020
Última revisión	28 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 4 portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco de Crédito e Inversiones (BCI), 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://csirt.gob.cl/alertas/8ffr20-00195-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00195-01.pdf

8FFR20-00196-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00196-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Enero de 2020
Última revisión	28 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Estado, 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://csirt.gob.cl/alertas/8ffr20-00196-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00196-01.pdf

8FFR20-00197-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00197-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Enero de 2020
Última revisión	28 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociado a una IP que suplanta el sitio web oficial de Banco Estado, 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://csirt.gob.cl/alertas/8ffr20-00197-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00197-01.pdf

8FFR20-00198-01 CSIRT ADVIERTE 6 SITIOS FRAUDULENTOS PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR20-00198-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Enero de 2020
Última revisión	29 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis portales fraudulentos asociados a tres IP que suplantan el sitio web oficial de Banco Estado, 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://csirt.gob.cl/alertas/8ffr20-00198-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00198-01.pdf

2CMV20-00043-01 CSIRT ADVIERTE DE MALWARE EN CORREO DE COMPAÑÍA DE TELECOMUNICACIONES

Alerta de seguridad informática	2CMV20-00043-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2020
Última revisión	25 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware que utiliza el nombre de la Compañía de Telecomunicaciones Entel.

El mensaje del correo indica que ha ocurrido un imprevisto en el pago de la cuenta del cliente, argumentando un problema asociado Rut denominado "valores en abierto". Al confuso mensaje se agrega un enlace a una factura, para la cual se solicita utilizar Windows. Al momento de seleccionar el enlace se descarga un archivo Zip. Al descomprimir el archivo se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado, se realiza un proceso falso de instalación, pero en realidad se gatilla un script que descarga el malware.

Enlace:

https://csirt.gob.cl/alertas/2cmv20-00043-01/
https://csirt.gob.cl/media/2020/01/2CMV20-00043-01.pdf

2CMV20-00044-01 CSIRT ADVIERTE DE CAMPAÑA PHISHING CON EMOTET

Alerta de seguridad informática	2CMV20-00044-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2020
Última revisión	27 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con malware Emotet.

La campaña consiste en el envío de un correo en idioma inglés cuyo mensaje hace alusión a una factura y un estado de cuenta, y cuyo pie de firma corresponde, supuestamente, a una empresa chilena. En el atacante trata de persuadir a la víctima para que seleccione el enlace. Al hacerlo se realiza la descarga de un archivo doc, el que una vez abierto desencadena una infección del malware comunicándose con otras URLs y servidores comando y control.

Enlace:

https://csirt.gob.cl/alertas/2cmv20-00044-01/
https://csirt.gob.cl/media/2020/01/2CMV20-00044-01.pdf

8FPH20-00097-01 CSIRT ADVIERTE DE PHISHING POR MANTENIMIENTO DE SERVICIOS BANCARIOS

Alerta de seguridad informática	8FPH20-00097-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Enero de 2020
Última revisión	24 de Enero de 2020

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 persuadir a los usuarios del Banco Estado.

El falso mensaje informa que se realizó un proceso de mantenimiento en los servicios de Caja Vecina, ServiEstado y aplicación móvil. Argumentando una supuesta política de seguridad, se le informa al cliente que el banco se vio obligado a bloquear su cuenta y que para reactivarla solo puede hacerlo a través del enlace que se dispone en el correo. Al seleccionar el vínculo, la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00097-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00097-01.pdf

8FPH20-00098-01 CSIRT ADVIERTE DE PHISHING BANCARIO SOBRE RETENCIÓN DE FONDOS

Alerta de seguridad informática	8FPH20-00098-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Enero de 2020
Última revisión	24 de Enero de 2020

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 clientes del Banco Scotiabank. En el mensaje los atacantes informan a la víctima sobre una supuesta transferencia de fondos retenida, acción que fue tomada por la propia seguridad del cliente. El phishing trata de persuadir a los usuarios para que revisan su estado de cuenta, lo que pueden realizar accediendo a un hipervínculo ubicado en el cuerpo del correo. Al seleccionar el enlace, el usuario es derivado a un sitio semejante al del banco.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00098-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00098-01.pdf

8FPH20-00099-01 CSIRT ADVIERTE DE PHISHING POR ACTUALIZACIÓN DE SERVICIOS

Alerta de seguridad informática	8FPH20-00099-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Enero de 2020
Última revisión	24 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico. El mensaje informa que se realizó un proceso de actualización de los servidores. Sin embargo, al realizar la actualización la cuenta del cliente fue bloqueada temporalmente. Para reactivar la cuenta el atacante disponibiliza un enlace en el cuerpo del correo. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00099-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00099-01.pdf

8FPH20-00100-01 CSIRT ADVIERTE DE PHISHING POR SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00100-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2020
Última revisión	27 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de la no verificación de la identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que es necesario que ingrese para verificar su información en la base de datos o de lo contrario se procederá al bloqueo de los servicios por internet. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales

Enlace:

https://csirt.gob.cl/alertas/8fph20-00100-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00100-01.pdf

8FPH20-00101-01 CSIRT ADVIERTE DE PHISHING DE SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00101-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2020
Última revisión	27 de Enero de 2020

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 engañar a los usuarios de la empresa de Streaming Netflix.

El correo indica que existe un problema con el monto de pago y solicita, a quien lo recibe, que normalice la situación lo antes posible para evitar problemas e interrupciones en el servicio. El atacante disponibiliza un enlace, que al ser seleccionarlo, redirige al usuario a un sitio semejante al de Netflix. En el sitio se solicita del usuario su nombre, número de tarjeta de crédito, fecha de caducidad y código de seguridad.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00101-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00101-01.pdf

8FPH20-00102-01 CSIRT ADVIERTE DE PHISHING POR CRÉDITO PRE-APROBADO

Alerta de seguridad informática	8FPH20-00102-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2020
Última revisión	27 de Enero de 2020

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 engañar a los usuarios del Banco de Chile.

El atacante utiliza un mensaje indicando que existe un crédito pre-aprobado de $500.000 pesos, de manera simple y sin papeleos. Esta promoción tiene una duración desde el 15 hasta el 30 de enero del 2020. Los estafadores disponibilizan un enlace para realizar la aprobación del crédito. Al seleccionar el enlace, la víctima es direccionada a un sitio semejante al del Banco de Chile.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00102-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00102-01.pdf

9VSA20-00127-01 CSIRT COMPARTE ACTUALIZACIONES DE SAMBA

Alerta de seguridad informática	9VSA20-00127-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Enero de 2020
Última revisión	23 de Enero de 2020

Vulnerabilidad

CVE-2019-14902
CVE-2019-14907
CVE-2019-19344

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Samba, referente a vulnerabilidades que afectan a su herramienta de servicios de archivos e impresiones para Microsoft, las cuales de ser explotadas permitirían a un atacante remoto (vía LAN) obtener recursos sensibles y realizar ataques de denegación de servicios, Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00127-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00127-01.pdf

9VSA20-00128-01 CSIRT COMPARTE ACTUALIZACIÓN PARA EL PLUG-IN DE WORDPRESS WPS HIDE LOGIN

Alerta de seguridad informática	9VSA20-00128-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2020
Última revisión	27 de Enero de 2020

Vulnerabilidad

En la función plugins_loaded, el complemento busca diferentes subcadenas en la variable de entorno REQUEST_URI utilizando la función strpos, y debido a que algunos REQUEST_URI no se decodifican con la función rawurldecode, un atacante podría codificar esas subcadenas en la URL para evadir la detección, provocando que complemento redirigiría al usuario a la página de inicio de sesión oculta.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información referente a una vulnerabilidad detectada en el plug-in de WordPress WPS Hide Login, complemento popular utilizado para ocultar la página de inicio de sesión predeterminada de WordPress (wp-login.php).

Enlace
https://csirt.gob.cl/vulnerabilidades/9vsa20-00128-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00128-01.pdf

9VSA20-00129-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR CISCO

Alerta de seguridad informática	9VSA20-00129-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2020
Última revisión	28 de enero de 2020

Vulnerabilidad
CVE-2019-15963
CVE-2019-16028
CVE-2020-3124
CVE-2019-15989
CVE-2019-16027
CVE-2019-16018
CVE-2019-16019
CVE-2019-16020
CVE-2019-16021
CVE-2019-16022
CVE-2019-16023
CVE-2019-16029
CVE-2019-12629
CVE-2020-3115
CVE-2019-12628
CVE-2019-12619
CVE-2020-3129
CVE-2019-16000
CVE-2020-3117
CVE-2020-3130
CVE-2020-3137
CVE-2020-3133
CVE-2020-3134
CVE-2020-3139
CVE-2020-3136
CVE-2019-1950
CVE-2020-3135
CVE-2020-3131
CVE-2020-3143
CVE-2020-3121
CVE-2020-3142
CVE-2019-12636

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a diversas vulnerabilidades que afectan a sus productos. El documento también incluye las mitigaciones correspondientes.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00129-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00129-01.pdf

9VSA20-00130-01 CSIRT COMPARTE ACTUALIZACIONES PARA FREEBSD

Alerta de seguridad informática	9VSA20-00130-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2020
Última revisión	21 de enero de 2020

Vulnerabilidad

CVE-2020-7450
CVE-2019-5613
CVE-2019-15875

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por FreeBSD referente a diversas vulnerabilidades que afectan a su sistema operativo.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00130-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00130-01.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante las pasadas dos semanas 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:

IoC	Motivo
93.231.229.200	Scan
77.247.108.243	Scan
183.88.228.100	Scan
89.218.157.102	Scan
80.82.77.41	Scan
51.68.176.189	Scan
36.39.68.34	Scan

150.242.74.90	Scan
116.86.205.193	Scan
89.38.145.19	Scan
182.55.229.126	Scan
201.159.251.253	Scan
164.160.22.202	Scan
58.182.130.161	Scan
193.227.20.168	Scan
181.50.99.8	Scan
195.231.4.32	Scan
185.53.88.119	Scan
185.172.110.220	Scan
187.16.145.180	phishing
185.53.88.120	Scan
188.138.70.92	Malware
188.241.58.209	Malware
208.83.20.20	Malware
212.47.227.58	Malware
5.206.3.65	Malware
50.23.35.196	Malware
50.23.35.220	Malware
50.23.4.234	Malware
50.23.4.238	Malware
62.138.0.158	Malware
72.20.16.242	Malware
75.126.18.148	Malware
78.142.18.61	Malware
80.29.66.86	Malware
81.201.61.196	Malware
87.233.192.213	Malware
113.176.123.110	Scan
103.224.182.251	Malware
173.193.103.184	Malware
173.193.113.227	Malware
173.193.113.229	Malware
173.193.113.236	Malware
173.193.113.251	Malware
173.193.113.253	Malware
89.144.47.246	Scan
184.105.151.164	Malware
184.173.23.84	Malware
184.173.23.88	Malware
184.173.25.73	Malware
184.173.25.75	Malware

184.173.3.23	Malware
184.173.3.26	Malware
184.173.3.45	Malware
184.173.3.46	Malware
184.173.3.5	Malware
103.79.143.225	Scan
105.96.52.117	Scan
159.65.174.81	Scan
159.89.154.19	Scan
193.57.40.38	Scan
195.225.198.198	Scan
209.141.37.159	Scan
36.71.234.135	Scan
77.247.110.45	Scan
80.211.246.150	Scan
103.99.1.35	Scan
88.85.69.189	Spam
209.53.113.223	Waledac.Botnet
104.18.28.160	phishing
192.185.5.44	phishing
167.172.208.19	Scan
104.156.255.79	Malware
190.152.125.22	Malware
149.154.67.19	Malware
101.108.92.111	Malware
103.63.31.38	Malware
193.26.212.24	Malware
128.201.174.107	Malware
195.93.223.100	Malware
131.161.253.190	Malware
144.91.79.12	Malware
144.91.79.9	Malware
145.239.188.93	Malware
200.116.199.10	Malware
170.233.120.53	Malware
200.127.121.99	Malware
200.21.51.38	Malware
178.183.150.169	Malware
201.187.105.123	Malware
181.10.207.234	Malware
201.210.120.239	Malware
181.49.61.237	Malware
212.22.75.95	Malware
185.117.75.112	Malware

31.128.13.45	Malware
185.222.202.192	Malware
31.214.138.207	Malware
185.62.188.117	Malware
45.235.213.126	Malware
186.71.150.23	Malware
45.66.10.22	Malware
187.58.56.26	Malware
45.67.231.164	Malware
188.225.82.68	Malware
46.174.235.36	Malware
190.111.255.219	Malware
81.190.160.139	Malware
190.13.160.19	Malware
106.12.69.27	Scan
124.156.134.179	Scan
45.136.109.122	Scan
185.232.65.111	Scan
134.209.203.65	Scan
45.67.14.153	Scan
157.245.251.195	Scan
103.99.1.245	Scan
213.202.211.81	Scan
89.34.27.133	DDoS
80.82.67.116	Scan
143.202.225.225	Scan
173.249.34.254	Scan
185.189.160.60	Scan
37.187.156.120	Scan
89.248.160.175	Scan
185.245.85.231	Scan
98.143.148.50	Scan
39.165.55.167	Scan
60.176.157.174	Scan
1.172.48.109	Scan
129.204.56.213	Scan
49.159.196.98	Scan
203.205.244.61	Scan
47.219.24.167	Scan
198.50.167.183	Scan
192.12.240.40	Scan
167.99.226.75	Scan
177.230.174.38	Scan
184.95.42.98	Scan

172.119.125.80	Scan
138.197.143.222	Scan
149.56.233.24	Scan
144.217.45.34	Scan
82.209.210.252	Scan
60.249.182.156	Scan
167.71.200.175	Scan
139.59.154.74	Scan
51.89.176.237	Scan
46.101.238.98	Scan
46.101.88.53	Scan
45.112.198.85	Scan
94.107.72.61	Scan
167.114.27.122	Scan
159.89.15.163	Scan
64.225.72.103	Scan
51.83.78.82	Scan
37.49.226.5	Scan
58.229.187.10	Scan
45.235.98.10	Scan
211.110.212.4	Scan
209.250.245.206	Scan
208.115.198.2	Scan
200.218.254.105	Scan
185.153.199.155	Scan
54.37.0.224	Scan
23.239.67.40	Scan
172.105.117.102	Scan
157.245.71.58	Scan
185.53.88.115	Scan
176.137.51.171	Scan
69.162.119.30	Scan
165.22.77.78	Scan
85.105.147.165	Scan
188.27.194.198	Scan
183.90.61.13	Scan
201.150.51.110	Scan
183.202.208.61	DdoS
27.217.148.143	DdoS
1.193.78.153	DdoS
42.115.216.117	DdoS
42.227.249.136	DdoS
118.74.116.250	DdoS
114.244.11.153	DdoS

39.179.86.49	DdoS
114.139.68.1	DdoS
59.64.129.2	DdoS
60.180.128.16	DdoS
171.105.168.40	DdoS
111.19.51.226	DdoS
111.22.240.139	DdoS
111.29.210.69	DdoS
115.51.15.224	DdoS
117.157.202.164	DdoS
123.133.95.141	DdoS
183.20.118.220	DdoS
36.47.128.0	DdoS
36.6.195.172	DdoS
60.6.219.150	DdoS
115.203.80.128	DdoS
123.170.150.138	DdoS
182.138.178.67	DdoS
188.94.68.228	Scan
188.14.108.197	Scan
188.166.54.163	Scan
167.172.163.85	Scan
207.154.198.18	Scan
89.163.224.233	Scan
157.245.66.227	Scan
92.4.170.48	Scan
167.172.163.143	Scan
157.230.105.113	Scan
167.172.163.76	Scan
216.144.240.162	Scan
139.59.46.226	Phishing
162.241.203.26	Phishing
216.245.211.42	Phishing
164.132.22.170	Scan
173.226.134.224	Scan
163.172.83.56	Scan
159.89.3.27	Scan
107.175.246.91	Scan
45.124.5.219	Scan
195.154.181.120	Scan
195.37.190.86	Scan
185.198.59.132	Scan
178.239.161.228	Scan
144.91.96.35	Scan

192.99.250.216	Scan
176.202.164.43	Scan
194.180.225.17	Scan
77.247.109.100	Scan
77.247.109.99	Scan
211.110.212.120	Scan
59.92.24.106	Scan
172.105.126.30	Scan
45.148.10.93	Scan
42.112.63.199	Scan
167.114.125.232	Scan
94.100.18.97	Malware
163.247.64.130	DdoS
178.63.11.228	Malware
80.211.6.36	Scan
223.179.131.129	Scan
63.250.36.8	Phishing
139.59.65.22	Phishing
37.49.231.145	Scan
103.206.130.84	Scan
202.152.24.234	Scan
193.56.28.30	Scan
202.166.217.97	Scan
180.246.59.148	Scan
192.3.8.162	Scan
178.128.83.204	Scan
172.104.87.194	Scan
139.59.43.104	Scan
104.248.143.17	Scan
85.208.186.251	Scan
167.99.0.78	Scan
185.53.88.15	Scan
168.149.138.72	Scan
46.166.187.111	Scan
185.134.22.95	Scan
185.89.126.3	Scan
122.181.22.42	Scan
79.117.115.124	Scan
116.86.149.43	Scan
86.105.145.148	Scan
62.215.91.24	Scan
45.231.195.197	Scan
103.232.39.241	Scan
45.143.220.189	Scan

107.2.42.98	Scan
54.39.209.226	Scan
207.180.236.85	Scan
185.234.216.19	DdoS
92.222.209.223	Scan
139.59.95.60	Phishing
143.137.32.7	Scan
157.119.73.71	DdoS
188.24.2.68	Scan
192.223.27.196	Scan
83.97.20.219	Scan
107.161.88.35	Scan
195.154.113.82	Scan
81.64.205.171	Scan
51.15.13.118	Scan
162.243.173.26	Scan
104.200.134.250	Scan
200.71.200.4	Emotet
200.69.93.166	Scan
131.0.86.249	Scan
195.22.26.248	Malware
163.247.52.14	Ransomware
163.247.45.18	Ransomware
141.98.10.136	Scan
103.138.109.160	Scan
77.247.110.37	Scan
68.183.85.198	Phishing
139.59.78.109	Phishing
206.189.158.0	Scan
196.202.220.249	Scan
194.75.90.80	Scan
185.231.223.8	Scan
31.7.62.44	DdoS
91.208.184.160	Scan
64.39.99.239	Scan
51.77.23.71	Scan
42.119.230.66	Scan
199.195.252.32	Scan
196.189.130.14	Scan
182.52.134.114	Scan
165.231.33.10	Scan

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos públicos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.
El CSIRT de gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Eduardo Aceto
- Andrés Basoalto

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: 2020.01.31 16:24:13 -03'00'