13BCS20-00045-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 13 de Marzo de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 05 y el miércoles 11 de Marzo de 2020.

Falsificación de Registro o Identidad

8FFR20-00241-01 CSIRT ADVIERTE DE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00241-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Marzo de 2020
Última revisión	05 de Marzo 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 del 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://www.csirt.gob.cl/alertas/8ffr20-00241-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00241-01.pdf

8FFR20-00242-01 CSIRT IDENTIFICÓ 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00242-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Marzo de 2020
Última revisión	05 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a una IP que suplanta el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00242-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00242-01.pdf

8FFR20-00243-01 CSIRT ADVIERTE DE 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00243-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Marzo de 2020
Última revisión	06 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00243-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00243-01.pdf

8FFR20-00244-01 CSIRT INFORMA DE 6 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00244-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Marzo de 2020
Última revisión	06 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00244-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00244-01-1.pdf

8FFR20-00245-01 CSIRT ADVIERTE DE 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00245-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Marzo de 2020
Última revisión	07 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00245-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00245-01.pdf

8FFR20-00246-01 CSIRT ADVIERTE DE 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00246-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Marzo de 2020
Última revisión	07 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs 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://www.csirt.gob.cl/alertas/8ffr20-00246-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00246-01.pdf

8FFR20-00247-01 CSIRT ADVIERTE DE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00247-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Marzo de 2020
Última revisión	07 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00247-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00247-01.pdf

8FFR20-00248-01 CSIRT IDENTIFICÓ UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00248-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Marzo de 2020
Última revisión	08 de Marzo 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 del Banco 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://www.csirt.gob.cl/alertas/8ffr20-00248-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00248-01.pdf

8FFR20-00249-01 CSIRT IDENTIFICÓ 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00249-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00249-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00249-01.pdf

8FFR20-00250-01 CSIRT ADVIERTE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00250-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00250-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00250-01.pdf

8FFR-00251-01 CSIRT INFORMA DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00251-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a dos IPs que suplanta el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr-00251-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00251-01.pdf

8FFR20-00252-01 CSIRT IDENTIFICÓ PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00252-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo 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 del 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://www.csirt.gob.cl/alertas/8ffr20-00252-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00252-01.pdf

8FFR20-00253-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00253-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 del 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://www.csirt.gob.cl/alertas/8ffr20-00253-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00253-01.pdf

8FFR20-00254-01 CSIRT IDENTIFICÓ UNA PÁGINA BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR20-00254-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 del 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://www.csirt.gob.cl/alertas/8ffr20-00254-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00254-01-1.pdf

8FFR20-00255-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00255-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 del 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://www.csirt.gob.cl/alertas/8ffr20-00255-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00255-01.pdf

8FFR20-00256-01 CSIRT IDENTIFICÓ 2 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00256-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00256-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00256-01.pdf

8FFR20-00257-01 CSIRT ADVIERTE DE 2 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00257-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo 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 suplantan el sitio web oficial del 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://www.csirt.gob.cl/alertas/8ffr20-00257-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00257-01.pdf

Malware

2CMV20-00051-01 CSIRT ADVIERTE MALWARE DE LIBERACIÓN DE PAGO A PENSIONADOS

Alerta de seguridad informática	2CMV20-00051-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware a través de un correo electrónico que utiliza el nombre de la Tesorería General de la República.

El mensaje del correo indica que según la información entregada en los noticieros del canal público, a partir del 27 de marzo de 2020 comenzará la liberación del pago a los pensionados por concepto de contribuciones e informa que los contribuyentes que han realizado sus pagos a tiempo serán premiados con un descuento del 70% durante 3 meses. El atacante intenta persuadir a la potencial víctima que solo a través del enlace adjunto y que ingresando su rut podrá saber si es beneficiario de este descuento. Al ingresar al enlace se descarga un archivo ZIP. Una vez que se descomprime 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://www.csirt.gob.cl/alertas/2cmv20-00051-01/

https://www.csirt.gob.cl/media/2020/03/2CMV20-00051-01.pdf

Phishing

8FPH20-00126-01 CSIRT IDENTIFICÓ PHISHING BANCARIO DE BLOQUEO O SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00126-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Marzo de 2020
Última revisión	06 de Marzo 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 Scotiabank. El atacante envía mensaje de diversos contenidos, como por ejemplo:

- Existe una operación irregular y que debe verificar
- Que la cuenta se encuentra suspendida por no realizar el pago de los impuestos
- Que se ha bloqueado su cuenta por realizar una operación sospechosa

De esa forma intenta persuadir al usuario que seleccione el enlace, al hacerlo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00126-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00126-01.pdf

8FPH20-00127-01 CSIRT ADVIERTE PHISHING DE REFINANCIAMIENTO DE DEUDAS

Alerta de seguridad informática	8FPH20-00127-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Marzo de 2020
Última revisión	09 de Marzo 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 que el banco le da la oportunidad de refinanciar las deudas con las tarjetas de crédito del Banco Estado y que tiene disponible un cupo de 2.890.000 pesos. Bajo ese argumento, el atacante intenta persuadir a la víctima de acceder a un enlace que se adjunta 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://www.csirt.gob.cl/alertas/8fph20-00127-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00127-01.pdf

8FPH20-00128-01 CSIRT ADVIERTE PHISHING DE CRÉDITO DE CONSUMO

Alerta de seguridad informática	8FPH20-00128-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Marzo de 2020
Última revisión	09 de Marzo 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 de Office Banking.

El mensaje informa que el banco le da la oportunidad de refinanciar las deudas con un crédito de consumo preaprobado con un cupo de hasta 9.440.000 pesos. Bajo ese argumento, el atacante intenta persuadir a la víctima de acceder a un enlace que se adjunta 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://www.csirt.gob.cl/alertas/8fph20-00128-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00128-01-1.pdf

8FPH20-00129-01 CSIRT ADVIERTE PHISHING DE TRANSFERENCIA RETENIDA

Alerta de seguridad informática	8FPH20-00129-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo 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 Scotiabank, indicando que existe una transferencia de retenida desde su cuenta. El atacante busca persuadir al usuario que seleccione el enlace para verificar el estado de cuenta, al hacerlo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00129-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00129-01.pdf

8FPH20-00130-01 CSIRT ADVIERTE PHISHING DE INCONVENIENTES CON EL DISPOSITIVO DE SEGURIDAD

Alerta de seguridad informática	8FPH20-00130-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo 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 Scotiabank, indicando que existe un inconveniente con el dispositivo de seguridad, por lo que se requiere sincronizar de manera inmediata. El atacante persuadir al usuario que seleccione el enlace para realizar la verificación del dispositivo, al hacerlo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00130-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00130-01.pdf

9VSA20-00151-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PRODUCTOS DE CISCO

Alerta de seguridad informática	9VSA20-00151-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Marzo de 2020
Última revisión	08 de Marzo de 2020

Vulnerabilidad

CVE-2020-3164
CVE-2020-3157
CVE-2020-3193
CVE-2020-3192
CVE-2020-3176
CVE-2020-3185
CVE-2020-3182
CVE-2020-3127
CVE-2020-3128
CVE-2020-3148
CVE-2020-3155
CVE-2020-3181
CVE-2020-3166
Vulnerabilidad
CVE-2020-3164

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.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00151-01-2/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00151-01.pdf

9VSA20-00152-01 CSIRT COMPARTE ACTUALIZACIÓN DE DJANGO

Alerta de seguridad informática	9VSA20-00152-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Marzo de 2020
Última revisión	09 de Marzo de 2020

Vulnerabilidad

CVE-2020-9402

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Django, referente a una vulnerabilidad que afecta a su marco de desarrollo web, la cual permitiría a un atacante remoto realizar inyecciones SQL. Este informe incluye su respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00152-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00152-01.pdf

9VSA-00153-001 CSIRT COMPARTE ACTUALIZACIONES PARA MICROSOFT

Alerta de seguridad informática	9VSA20-00153-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

Vulnerabilidad

Reportados en el informe de marzo:
CVE-2020-0765
CVE-2020-0774
CVE-2020-0775
CVE-2020-0795
CVE-2020-0813
CVE-2020-0820
CVE-2020-0850
CVE-2020-0851
CVE-2020-0852
CVE-2020-0853
CVE-2020-0855
CVE-2020-0859
CVE-2020-0861
CVE-2020-0863
CVE-2020-0871
CVE-2020-0874
CVE-2020-0876
CVE-2020-0879
CVE-2020-0880
CVE-2020-0882
CVE-2020-0885
CVE-2020-0891
CVE-2020-0892
CVE-2020-0893
CVE-2020-0894

CVE-2020-0902

Reportado adicionalmente:

ADV200005
CVE-2020-0645
CVE-2020-0684
CVE-2020-0690
CVE-2020-0700
CVE-2020-0758
CVE-2020-0762
CVE-2020-0763
CVE-2020-0768
CVE-2020-0769
CVE-2020-0770
CVE-2020-0771
CVE-2020-0772
CVE-2020-0773
CVE-2020-0776
CVE-2020-0777
CVE-2020-0778
CVE-2020-0779
CVE-2020-0780
CVE-2020-0781
CVE-2020-0783
CVE-2020-0785
CVE-2020-0786
CVE-2020-0787
CVE-2020-0788
CVE-2020-0789
CVE-2020-0791
CVE-2020-0793
CVE-2020-0797
CVE-2020-0798
CVE-2020-0799
CVE-2020-0800
CVE-2020-0801
CVE-2020-0802
CVE-2020-0803
CVE-2020-0804
CVE-2020-0806
CVE-2020-0807
CVE-2020-0808
CVE-2020-0809
CVE-2020-0810
CVE-2020-0811
CVE-2020-0812

CVE-2020-0814
CVE-2020-0815
CVE-2020-0816
CVE-2020-0819
CVE-2020-0822
CVE-2020-0823
CVE-2020-0824
CVE-2020-0825
CVE-2020-0826
CVE-2020-0827
CVE-2020-0828
CVE-2020-0829
CVE-2020-0830
CVE-2020-0831
CVE-2020-0832
CVE-2020-0833
CVE-2020-0834
CVE-2020-0840
CVE-2020-0841
CVE-2020-0842
CVE-2020-0843
CVE-2020-0844
CVE-2020-0845
CVE-2020-0847
CVE-2020-0848
CVE-2020-0849
CVE-2020-0854
CVE-2020-0857
CVE-2020-0858
CVE-2020-0860
CVE-2020-0864
CVE-2020-0865
CVE-2020-0866
CVE-2020-0867
CVE-2020-0868
CVE-2020-0869
CVE-2020-0872
CVE-2020-0877
CVE-2020-0881
CVE-2020-0883
CVE-2020-0884
CVE-2020-0887
CVE-2020-0896
CVE-2020-0897
CVE-2020-0898

CVE-2020-0903
CVE-2020-0905

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 marzo de 2020, parchando 26 vulnerabilidades en sus softwares, además se informa de 89 vulnerabilidades adicionales al reporte mensual.
Un aviso importante además de las actualizaciones es un reporte (ADV200005) referente al servicio SMBv3 en el cual posee una vulnerabilidad aún no parchada, sin embargo, Microsoft recomienda una solución alterna. En este informe se dará un breve detalle de lo reportado por Microsoft.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00153-001/
https://www.csirt.gob.cl/media/2020/03/9VSA-00153-001.pdf

9VSA20-00154-01 CSIRT COMPARTE ACTUALIZACIÓN DE MOZILLA PARA FIREFOX Y FIREFOX ESR

Alerta de seguridad informática	9VSA20-00154-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Marzo de 2020
Última revisión	04 de Marzo de 2020

Vulnerabilidad

CVE-2020-6805
CVE-2020-6806
CVE-2020-6807
CVE-2020-6808
CVE-2020-6809
CVE-2020-6810
CVE-2020-6811
CVE-2020-6812
CVE-2020-6813
CVE-2020-6814
CVE-2020-6815
CVE-2019-20503

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Mozilla, referente a vulnerabilidades que afectan a sus exploradores Firefox y Firefox ESR, las cuales, de ser explotadas, permitirían a un atacante remoto comprometer completamente al sistema afectado. Este informe incluye su respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00154-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00154-01.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
192.241.225.220	Port Scan
192.241.224.176	Port Scan
192.241.221.122	Port Scan
198.54.113.6	Port Scan
192.241.222.149	Port Scan
45.114.116.121	Port Scan
192.241.224.192	Port Scan
192.241.222.82	Port Scan
198.199.101.131	Port Scan
192.241.234.131	Port Scan
165.22.209.25	Phishing
192.241.209.130	Port Scan
192.241.225.236	Port Scan
104.18.51.227	Phishing
104.18.50.227	Phishing
160.153.137.210	Phishing
47.245.32.253	Phishing
192.241.217.174	Port Scan
192.241.218.213	Port Scan
192.241.221.36	Port Scan
192.241.226.155	Port Scan
192.241.229.148	Port Scan
192.241.233.184	Port Scan
192.241.228.8	Port Scan
192.241.229.119	Port Scan
192.241.216.109	Port Scan
192.241.215.82	Port Scan
192.241.223.98	Port Scan
192.241.230.45	Port Scan
192.241.232.146	Port Scan
192.241.209.194	Port Scan

192.241.210.98	Port Scan
192.241.227.83	Port Scan
188.165.214.134	Port Scan
192.241.233.180	Port Scan
192.241.235.28	Port Scan
192.241.219.144	Port Scan
192.241.228.40	Port Scan
192.241.219.116	Port Scan
192.241.225.197	Port Scan
192.241.212.26	Port Scan
209.99.40.222	Phishing
209.99.40.223	Phishing
54.37.241.234	Port Scan
80.82.65.234	Port Scan
192.241.221.137	Port Scan
45.113.122.172	Malware
192.241.224.129	Port Scan
192.241.231.197	Port Scan
45.13.252.133	Phishing
45.155.37.115	Phishing
192.241.222.7	Port Scan
192.241.222.5	Port Scan
192.241.213.149	Port Scan
199.191.50.188	Malware
192.241.214.144	Port Scan
192.241.224.234	Port Scan
192.241.227.40	Port Scan
192.241.217.171	Port Scan
192.241.208.59	Port Scan
192.241.214.172	Port Scan
192.241.224.73	Port Scan
192.241.231.130	Port Scan
64.32.7.74	Port Scan
206.221.176.103	Port Scan
51.83.66.171	Port Scan
192.241.226.236	Port Scan
192.241.223.243	Port Scan
198.199.96.178	Port Scan
149.202.139.194	Port Scan
192.241.227.151	Port Scan
192.241.210.71	Port Scan

192.241.214.109	Port Scan
192.241.219.121	Port Scan
45.143.220.98	Port Scan
125.17.138.42	Port Scan
27.200.41.222	DDoS
119.39.95.16	DDoS
171.43.165.149	DDoS
27.18.122.21	DDoS
183.200.230.3	DDoS
112.42.142.50	DDoS
183.163.211.221	DDoS
36.40.232.215	DDoS
101.87.184.59	DDoS
183.198.2.211	DDoS
192.241.228.88	Port Scan
192.241.207.208	Port Scan
192.241.226.105	Port Scan
192.241.227.7	Port Scan
192.241.212.113	Port Scan
192.241.218.98	Port Scan
192.241.227.78	Port Scan
192.241.220.130	Port Scan
198.199.98.199	Port Scan
192.241.222.41	Port Scan
202.72.221.170	Port Scan
192.241.224.47	Port Scan
192.241.227.85	Port Scan
45.143.220.208	Port Scan
192.241.219.107	Port Scan
192.241.226.191	Port Scan
192.241.223.96	Port Scan
192.241.208.177	Port Scan
192.241.212.246	Port Scan
192.241.227.251	Port Scan
192.241.219.236	Port Scan
192.241.213.213	Port Scan
192.241.233.166	Port Scan
192.241.207.126	Port Scan
198.199.114.219	Port Scan
192.241.220.92	Port Scan
192.241.198.223	Port Scan

192.241.228.76	Port Scan
192.241.230.7	Port Scan
192.241.222.97	Port Scan
192.241.212.158	Port Scan
93.174.93.143	Port Scan
192.241.214.40	Port Scan
192.241.219.128	Port Scan
192.241.234.183	Port Scan
192.241.233.39	Port Scan
192.241.232.66	Port Scan
171.247.167.122	Port Scan
192.99.91.240	Port Scan
117.68.208.57	Port Scan
120.244.131.6	Port Scan
112.132.182.99	Port Scan
27.17.211.15	Port Scan
125.81.158.154	Port Scan
171.41.51.58	Port Scan
180.105.241.150	Port Scan
117.182.109.244	Port Scan
1.80.243.146	Port Scan
113.222.183.247	Port Scan
45.143.220.11	Port Scan
156.67.53.154	Port Scan
192.241.208.6	Port Scan
192.241.217.63	Port Scan
192.241.223.22	Port Scan
192.241.216.200	Port Scan
192.241.225.110	Port Scan
192.241.226.18	Port Scan
185.53.88.48	Port Scan
192.241.234.193	Port Scan
192.241.233.20	Port Scan
192.241.216.100	Port Scan
192.241.226.142	Port Scan
192.241.208.92	Port Scan
192.241.214.64	Port Scan
134.73.206.2	Port Scan
185.53.88.43	Port Scan
194.9.70.248	Port Scan
83.97.20.213	Port Scan

192.241.229.252	Port Scan
192.241.216.147	Port Scan
192.241.207.57	Port Scan
192.241.209.231	Port Scan
192.241.227.160	Port Scan
192.241.233.83	Port Scan
45.143.220.238	Port Scan
192.241.222.163	Port Scan
192.241.222.181	Port Scan
192.241.231.29	Port Scan
192.241.227.93	Port Scan
192.241.207.195	Port Scan
185.177.59.115	Malware
192.241.223.185	Port Scan
192.241.229.239	Port Scan
192.241.204.232	Port Scan
192.241.233.251	Port Scan
103.241.227.107	Hacking
182.160.99.242	Hacking
167.172.252.251	Hacking
191.7.212.66	Hacking
217.64.109.231	Hacking
186.248.146.170	Hacking
192.241.204.232	Port Scan
192.241.206.133	Port Scan
185.39.10.14	Port Scan
192.241.235.85	Port Scan
192.241.209.238	Port Scan
192.241.221.89	Port Scan
192.241.218.35	Port Scan
83.191.180.7	Hacking
62.171.132.70	Hacking
85.33.39.225	Hacking
186.148.38.230	Hacking
177.10.104.117	Hacking
192.241.220.104	Port Scan
105.174.36.206	Port Scan
103.85.228.33	Port Scan
187.85.13.35	Port Scan
78.170.32.84	Port Scan
168.194.251.124	Port Scan

192.241.209.221	Port Scan
192.241.224.186	Port Scan
192.241.227.243	Port Scan
103.141.136.221	Port Scan
185.43.209.194	Port Scan
192.241.204.239	Port Scan
192.241.206.218	Port Scan
192.241.226.237	Port Scan
192.241.226.24	Port Scan
23.237.182.202	Port Scan
63.143.35.230	Port Scan
182.75.176.107	Hacking
201.229.156.107	Hacking
107.180.112.86	Phishing
192.241.204.128	Port Scan
14.39.153.119	Port Scan
198.98.62.43	Port Scan
103.35.65.54	Port Scan
192.241.230.58	Port Scan
192.241.211.238	Port Scan
192.241.205.20	Port Scan
198.98.62.43	Port Scan
192.241.225.14	Hacking
192.241.227.122	Hacking
185.173.35.53	Port Scan
74.82.47.23	Port Scan
45.76.17.124	Port Scan
192.241.210.136	Hacking
144.202.60.122	Port Scan
192.241.222.234	Port Scan
192.241.210.232	Port Scan
192.241.210.120	Port Scan
192.241.231.199	Port Scan
192.241.213.181	Port Scan
192.241.230.101	Port Scan
209.126.103.59	Malware
156.65.147.70	Port Scan
46.246.39.165	Port Scan
177.155.36.254	Port Scan
45.33.69.170	Port Scan
45.51.18.203	Port Scan

45.33.71.134	Port Scan
138.197.168.163	Port Scan
45.33.64.113	Port Scan
1.20.221.190	Port Scan
49.48.241.209	Port Scan
14.231.191.230	Port Scan
110.77.244.105	Port Scan
188.14.112.149	Port Scan
113.30.248.56	Port Scan
192.241.223.27	Port Scan
192.241.220.220	Port Scan
192.241.211.34	Port Scan
192.241.221.27	Port Scan
198.199.94.210	Port Scan
192.241.227.204	Port Scan
192.241.221.99	Port Scan
45.143.220.248	Port Scan
192.241.232.238	Port Scan
139.59.64.223	Phishing
192.241.223.237	Port Scan
192.241.232.99	Port Scan
194.55.132.234	Port Scan
81.169.206.128	Port Scan
181.99.188.46	Port Scan
62.219.118.129	Port Scan
145.14.144.21	Phishing
186.10.224.138	DDoS

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: 2020.03.12 17:42:16 -03'00'