CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 10 de Enero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 02 de y el miércoles 08 de Enero de 2020.

Falsificación de Registro o Identidad

8FFR20-00171-01 CSIRT ADVIERTE ACTIVACIÓN DE 3 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00171-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Enero de 2020
Última revisión	03 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://www.csirt.gob.cl/alertas/8fph20-00082-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00171-01.pdf

8FFR20-00172-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00172-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2020
Última revisión	05 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 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/8ffr20-00172-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00172-01.pdf

8FFR20-00173-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00173-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Enero de 2020
Última revisión	05 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://www.csirt.gob.cl/alertas/8ffr20-00173-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00173-01.pdf

8FFR20-00174-01 CSIRT ADVIERTE ACTIVACIÓN DE 7 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00174-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2020
Última revisión	07 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Scotiabank, los que podrían 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/8ffr20-00174-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00174-01.pdf

8FFR20-00175-01 CSIRT ADVIERTE DE CUATRO PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00175-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2020
Última revisión	08 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Scotiabank, los que podrían 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/8ffr20-00175-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00175-01.pdf

8FFR20-00176-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00176-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2020
Última revisión	08 de Enero 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 suplantan el sitio web oficial de Banco Estado, los que podrían 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/8ffr20-00176-01/
https://www.csirt.gob.cl/media/2020/01/8FFR20-00176-01.pdf

8FFR20-00177-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00177-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2020
Última revisión	08 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://www.csirt.gob.cl/alertas/8ffr20-00177-01/
https://www.csirt.gob.cl/media/2020/01/8FFR20-00177-01.pdf

8FFR20-00178-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00178-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Enero de 2020
Última revisión	09 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 suplantan el sitio web oficial de Banco Estado, los que podrían 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/8ffr20-00178-01/
https://www.csirt.gob.cl/media/2020/01/8FFR20-00178-01.pdf

Phishing

8FPH20-00080-01 CSIRT ADVIERTE DE CAMPAÑA DE PHISHING EN SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00080-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Enero de 2020
Última revisión	02 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 se realizó un bloqueo temporal de la membresía para mantener la cuenta segura y se debe reactivarla la cuenta dentro de las 24 horas. Los estafadores disponibilizan un enlace para restaurar la cuenta, incitando a sus víctimas a ingresar al vínculo. El enlace lo direcciona a un sitio semejando al de la empresa Netflix, donde los atacantes solicitan a sus víctimas los datos de sus cuentas y luego los redireccionan a una nueva página para solicitar los datos de la tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00080-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00080-01.pdf

8FPH20-00082-01 CSIRT INFORMA DE PHISHING BANCARIO POR TRANSFERENCIA RETENIDA DE FONDOS

Alerta de seguridad informática	8FPH20-00082-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Enero de 2020
Última revisión	03 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 Scotiabank para seleccionar un hipervínculo que los direcciona a un sitio semejante al del Banco. Para ello, el atacante utiliza un mensaje indicando que existe una transferencia de fondos retenida y así convencer a la víctima de seleccionar el enlace.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00082-01-2/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00082-01.pdf

8FPH20-00083-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING POR MANTENIMIENTO DE SERVICIOS

Alerta de seguridad informática	8FPH20-00083-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Enero de 2020
Última revisión	03 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, comunicando a as potenciales víctimas sobre la realización de un mantenimiento en los servicios de Caja Vecina, Servi Estado y en la aplicaciones móviles, por un error en la cuenta. Por ese motivo, informan los atacantes, se procedió al bloqueo de la cuenta. Los atacantes utilizan un mensaje para que la víctima active su cuenta, quien al seleccionar el enlace es direccionado a un sitio semejante al del Banco.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00083-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00083-01.pdf

8FPH20-00084-01 CSIRT ADVIERTE DE PHISHING POR BLOQUEO DE CUENTA

Alerta de seguridad informática	8FPH20-00084-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2020
Última revisión	04 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 mensaje por correo electrónico dirigido a los usuarios del Banco Estado. El mensaje advierte a las víctimas sobre la realización de un mantenimiento en los servicios de Caja Vecina, Servi Estado y en las aplicaciones móviles. Producto de lo anterior, se produjo un bloqueo de la cuenta, el que para ser corregido, el atacante exige al usuario reactivar su cuenta desde el mail, ingresar sus datos en un enlace adjunto. Al seleccionar el enlace, el usuario es direccionado a un sitio semejante al del Banco.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00084-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00084-01.pdf

8FPH20-00085-01 CSIRT ADVIERTE DE CORREO DE PHISHING DE FONDOS MUTUOS

Alerta de seguridad informática	8FPH20-00085-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Enero de 2020
Última revisión	04 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 Estado, en especial del servicio de Fondos Mutuos. El mensaje informa a las potenciales víctimas sobre un error en el sistema que derivó en la suspensión de la cuenta producto de la no verificación de su identidad. El atacante dispone de un enlace para que la víctima restablezca su acceso a las cuentas.

En el mensaje, cuya redacción es menos sofisticada de lo habitual, el atacante tiene la audacia de informar sobre las medidas de seguridad del servicio, como la encriptación de la cartola.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00085-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00085-01.pdf

8FPH20-00086-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING EN SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00086-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 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 advierte sobre un eventual problema para procesar el método de pago. El atacante solicita actualizar la información de la cuentapara enmendar la situación, facilitando a su víctima un enlace para actualizar su cuenta. Al seleccionar el enlace, la persona es redireccionada a un sitio semejante al de la empresa Netflix.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00086-01/

https://www.csirt.gob.cl/media/2020/01/8FPH20-00086-01.pdf

8FPH20-00087-01 CSIRT ADVIERTE DE CAMPAÑA DE PHISHIG EN CORREO CORPORATIVO

Alerta de seguridad informática	8FPH20-00087-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 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 engañar a los usuarios del correo electrónico corporativo Zimbra.

El correo informa sobre una supuesta expiración de contraseña en 2 días. Para evitar que esto suceda, el usuario debe seleccionar el enlace adjunto. Al seleccionar “Conserve mi cuenta”, la víctima es dirigida a un sitio falso del correo corporativo donde se le solicita el nombre de usuario y contraseña.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00087-01/

https://www.csirt.gob.cl/media/2020/01/8FPH20-00087-01.pdf

8FPH20-00088-01 CSIRT ADVIERTE DE PHISHING DE CADENA DE SUPERMERCADO VÍA WHATSAPP

Alerta de seguridad informática	8FPH20-00088-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing vía WhatsApp, indicando a quienes lo reciben que el supermercado Lider se encuentra de aniversario y, como promoción especial, está regalando un cupón de $50.000 pesos para celebrar. El atacante disponibiliza un vínculo para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionado a un sitio semejante al del supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades en WhatsApp (20 amigos o 5 grupos), acción necesaria para obtener su cupón.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00088-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00088-01.pdf

8FPH20-00089-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING DE SUPERMERCADO VÍA WHATSAPP

Alerta de seguridad informática	8FPH20-00089-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Enero de 2020
Última revisión	06 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing vía WhatsApp, indicando a quienes lo reciben que el supermercado Jumbo se encuentra de aniversario y, como promoción especial, está regalando un cupón de $50.000 pesos para celebrar. El atacante disponibiliza un vínculo para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionado a un sitio semejante al del supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades en WhatsApp (20 amigos o 5 grupos), acción necesaria para obtener su cupón.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00089-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00089-01.pdf

8FPH20-00090-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR CRÉDITO PRE-APROBADO

Alerta de seguridad informática	8FPH20-00090-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2020
Última revisión	07 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 a la potencial víctima sobre la existencia de un crédito pre-aprobado de $500.000 pesos disponible, de manera simple y sin papeleos. Esta promoción tiene una duración desde el 1 hasta el 15 de enero del 2020. En el mensaje, los estafadores disponibilizan un enlace a través del cual se aprueba le crédito. Al seleccionar el enlace, la persona es direccionada a un sitio semejante al del Banco.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00090-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00090-01.pdf

SMiShing

8FPH20-00081-01 CSIRT ADVIERTE DE CAMPAÑA DE SMISHING EN SERVICIO DE STREAMING DE MÚSICA

Alerta de seguridad informática	8FPH20-00081-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Enero de 2020
Última revisión	02 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de SMiShing a través de un mensaje de texto que intenta engañar a los usuarios del servicio streaming de música Spotify.

El mensaje indica a la potencial víctima que la subscripción del servicio premiun fue cancelado, disponiendo como alternativa, para volver a recibir el servicio, ingresar al enlace dispuesto en el mensaje. Al ingresar al enlace, la persona es derivada a una interfaz que simula ser el aplicativo oficial del servicio en el que solicita las credenciales del cliente. Enseguida, la persona es enviada a una nueva página del sitio donde son capturadas sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00081-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00081-01.pdf

Malware

2CMV20-00041-01 CSIRT ADVIERTE DE MALWARE QUE UTILIZA NOMBRE DE TESORERÍA

Alerta de seguridad informática	2CMV20-00041-01
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2020
Última revisión	08 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración del usuario @JosePablo_PUQ, han identificado una campaña de malware que utiliza el nombre de la Tesorería General de la Republica.

El mensaje del malware, alojado en un sitio fraudulento, informa a la víctima que existen obligaciones tributarias impagas detectados por el SII.

La amenaza se pudo identificar en un sitio web, el cual, al momento de ingresar, automáticamente descarga el archivo ZIP. Al descomprimir el archivo se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado se gatilla un script que descarga del malware

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00041-01/

https://www.csirt.gob.cl/media/2020/01/2CMV20-00041-01.pdf

Vulnerabilidades

9VSA20-00111-01 CSIRT COMPARTE ACTUALIZACIONES PARA AVIRA

Alerta de seguridad informática	9VSA20-00111-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Enero de 2020
Última revisión	02 de Enero de 2020

Vulnerabilidad

CVE-2019-18568

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Avira referente a una vulnerabilidad que afecta a su software Antivirus, la cual, si es explotada, puede resultar en la escalación de privilegios en el sistema víctima. El informe incluye la respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00111-01/

https://csirt.gob.cl/media/2020/01/9VSA20-00111-01.pdf

9VSA20-00112-01 CSIRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS CISCO

Alerta de seguridad informática	9VSA20-00112-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de enero de 2020
Última revisión	03 de enero de 2020

Vulnerabilidad

CVE-2019-15999
CVE-2019-15983
CVE-2019-15978
CVE-2019-15979
CVE-2019-15980
CVE-2019-15981
CVE-2019-15982
CVE-2019-15984
CVE-2019-15985
CVE-2019-15975
CVE-2019-15976
CVE-2019-15977

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a vulnerabilidades que afectan a sus productos.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00112-01/
https://www.csirt.gob.cl/media/2020/01/9VSA20-00112-01.pdf

9VSA20-00113-01 CSIRT COMPARTE ACTUALIZACIONES PARA MICROSOFT SHAREPOINT

Alerta de seguridad informática	9VSA20-00113-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de enero de 2020
Última revisión	07 de enero de 2020

Vulnerabilidad

CVE-2019-1491

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Microsoft, referente a una vulnerabilidad que afecta su herramienta de colaboración empresarial, Microsoft SharePoint. De ser explotada la vulnerabilidad, permitiría a un atacante remoto obtener información confidencial. El informe incluye la respectiva mitigación entregada por el proveedor.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00113-01/
https://www.csirt.gob.cl/media/2020/01/9VSA20-00113-01.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
45.143.220.151	Port Scan
81.177.143.31	DDoS
113.53.18.24	Port Scan
202.182.100.182	Port Scan
51.89.173.198	Port Scan
14.245.132.67	Port Scan
79.148.90.204	Port Scan
163.172.106.188	Port Scan
178.125.128.236	Port Scan
189.122.22.104	Port Scan
94.176.148.78	Port Scan
156.96.151.226	Port Scan
68.183.115.211	Port Scan
210.56.59.70	Port Scan
159.138.233.254	Port Scan
163.152.175.192	Port Scan
196.195.87.93	Port Scan
196.195.88.106	Port Scan
196.195.88.108	Port Scan
196.195.88.65	Port Scan
54.38.31.0	Port Scan
89.38.145.86	Port Scan
187.33.94.82	Port Scan
144.202.72.194	Port Scan
149.56.14.86	Port Scan
205.185.117.232	Port Scan
45.95.168.139	Port Scan
51.77.109.116	Port Scan
49.145.194.121	Port Scan

112.157.62.185	Port Scan
113.160.142.210	Port Scan
202.182.124.179	Port Scan
144.91.80.99	Port Scan
77.247.109.56	Port Scan
178.238.236.128	Port Scan
103.21.151.217	Port Scan
205.209.162.125	Port Scan
185.153.197.139	Port Scan
118.175.219.35	Port Scan
113.176.84.150	Port Scan
103.217.177.134	Port Scan
199.195.254.145	Port Scan
27.72.31.181	Port Scan
209.97.142.190	Port Scan
185.12.178.11	Port Scan
118.175.219.35	Port Scan
178.79.144.120	Port Scan
77.247.110.15	Port Scan
212.237.46.26	Port Scan
51.89.39.181	Malware
23.94.184.109	Malware
198.251.83.184	Port Scan
178.79.173.181	Port Scan
196.6.105.184	Port Scan
163.22.60.4	Port Scan
113.183.102.10	Port Scan
195.7.0.37	Port Scan
89.46.72.246	Port Scan
217.217.49.49	Port Scan
58.182.172.120	Port Scan
45.163.78.150	Port Scan
58.182.153.163	Port Scan
109.160.72.196	Port Scan
39.109.136.160	Port Scan
107.180.27.138	Spam
58.182.71.245	Port Scan
58.182.84.15	Port Scan
178.159.36.146	Spam
185.81.154.5	Port Scan
175.201.64.187	Port Scan

212.237.46.133	Port Scan
47.56.66.163	Port Scan
81.215.3.193	Port Scan
221.156.173.85	Port Scan
119.195.152.115	Port Scan
14.63.55.161	Port Scan
221.156.173.85	DDoS
119.195.152.115	DDoS
14.63.55.181	DDoS
78.23.10.104	DDoS
176.113.70.62	Port Scan
175.201.64.185	Port Scan
78.23.10.104	Port Scan
80.82.78.96	Port Scan
185.56.80.40	Port Scan
64.44.40.66	Port Scan
181.188.133.50	Port Scan
117.239.128.186	Port Scan
37.49.231.168	Port Scan
1.231.60.35	Port Scan
222.236.58.11	Port Scan
115.23.89.252	Port Scan
59.3.245.10	Port Scan
118.40.82.19	Port Scan
121.168.192.234	Port Scan
120.29.133.46	Port Scan
3.81.9.20	Port Scan
202.133.59.91	Port Scan
1.227.188.110	Port Scan
37.49.231.106	Port Scan
58.231.118.227	Port Scan
59.6.14.212	Port Scan
59.6.14.230	Port Scan
93.104.209.17	Port Scan
61.80.153.98	Port Scan
109.95.90.75	Port Scan
121.179.149.105	Port Scan
122.40.8.67	Port Scan
176.67.76.247	Port Scan
210.113.198.107	Port Scan
210.179.154.227	Port Scan

220.80.65.161	Port Scan
220.80.138.118	Port Scan
80.82.64.229	Port Scan
125.25.219.2	Port Scan
51.89.119.53	Port Scan
43.249.113.202	Port Scan
51.159.55.54	Port Scan
123.18.13.149	Port Scan
111.125.221.58	Port Scan
91.105.92.254	Port Scan
172.104.82.242	Port Scan
104.248.142.122	Port Scan
5.188.206.22	Port Scan
109.93.81.66	Port Scan
178.62.41.236	Port Scan
185.173.35.33	Port Scan
209.141.62.7	Port Scan
199.231.184.237	Port Scan
178.62.108.111	Port Scan
138.197.99.20	Port Scan
62.12.114.241	Port Scan
54.36.185.102	Port Scan
51.158.24.196	Port Scan
163.172.104.209	Port Scan
68.183.123.226	Port Scan
27.79.154.172	Port Scan
192.169.82.54	Port Scan
47.244.138.235	Port Scan
51.77.110.48	Port Scan
70.177.115.60	Port Scan
197.55.69.14	Port Scan
199.19.56.1	Port Scan
199.19.53.1	Port Scan
199.19.54.1	Port Scan
198.97.190.53	Port Scan
199.249.120.1	Port Scan
199.19.57.1	Port Scan
114.134.22.250	Port Scan
37.148.211.38	Port Scan
91.134.127.236	Port Scan
192.99.209.235	Port Scan

37.49.230.93	Port Scan
189.51.193.102	Port Scan
201.159.180.246	Port Scan
188.166.27.140	Port Scan
24.237.86.44	Port Scan
205.209.158.47	Port Scan
51.89.229.158	Port Scan
202.51.102.236	Port Scan
45.32.149.97	Port Scan
193.226.218.75	Port Scan
165.227.86.48	Port Scan
144.217.85.239	Port Scan
174.138.34.166	Port Scan
94.247.130.194	Port Scan
202.138.239.252	Port Scan
170.79.88.6	Port Scan
138.201.90.85	Port Scan
74.64.186.216	Port Scan
204.101.47.115	Port Scan
37.49.231.101	Port Scan
68.183.74.100	Port Scan
171.231.75.215	Port Scan
113.160.72.154	Port Scan
103.99.2.4	Port Scan
51.38.150.34	Port Scan
157.245.202.221	Port Scan
190.104.149.195	Port Scan
91.231.211.154	Port Scan
36.78.132.47	Port Scan
212.233.180.38	Port Scan
103.26.221.223	Port Scan
182.19.200.48	Port Scan
58.182.8.46	Port Scan
35.245.169.238	Port Scan
69.88.157.139	Port Scan
98.223.53.70	Port Scan
201.35.195.208	Port Scan
31.14.40.246	Port Scan
121.121.94.21	Port Scan
31.14.40.246	Port Scan
93.114.130.135	Port Scan

117.7.236.35	Port Scan
192.252.184.194	Port Scan
131.72.108.2	Port Scan
103.53.168.112	Port Scan
51.79.31.74	Port Scan
198.50.194.17	Port Scan
103.207.37.151	Port Scan
185.53.88.46	Port Scan
122.3.159.185	Port Scan
128.199.220.232	Port Scan
93.104.215.103	Port Scan
163.172.128.177	Port Scan
196.168.164.202	Port Scan
54.38.239.58	Port Scan
112.6.33.59	DDoS
111.182.110.52	DDoS
122.230.135.94	DDoS
36.63.11.14	DDoS
111.173.136.94	DDoS
45.113.192.202	DDoS
95.172.68.64	DDoS
95.172.68.62	DDoS
95.172.68.56	DDoS
201.236.92.101	DDoS
80.82.78.100	DDoS
190.171.156.236	DDoS
200.54.219.147	DDoS
200.111.196.124	DDoS
186.10.227.242	DDoS
190.54.38.234	DDoS
186.10.239.182	DDoS
186.67.39.27	DDoS
186.67.188.130	DDoS
186.10.24.210	DDoS
200.68.36.10	DDoS
221.218.160.168	DDoS
221.213.12.204	DDoS
119.176.66.186	DDoS
114.221.181.148	DDoS
117.143.104.205	DDoS
113.100.219.36	DDoS

113.9.192.154	DDoS
125.70.177.19	DDoS
110.72.242.251	DDoS
218.85.232.40	DDoS
182.148.200.235	DDoS
190.164.55.133	DDoS
139.59.13.13	Phishing

URL's	Motivo
bloqueo-bancoestado[.]ddns[.]net	Phishing
https[:]//pollachilena.servicioalclientes.online/	Phishing
https[:]//www1.acceso.scotia.cl.no-cache.info/login/personas/	Phishing
http://www[.]rocketbroadband[.]ie/in/www.bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas.html	Phishing
http://hoitinhocxaydung.vn/shit/imagenes/comun2008/banca-en-linea-personas.html	Phishing

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.

- Tomás Gaete - https://www.linkedin.com/in/tomas-gaete-b8a2208b/
- Jair Palma - https://www.linkedin.com/in/jair-palma-vicenty-62038920/
- José Vásquez - https://www.linkedin.com/in/josé-francis-vasquez-garcia-52934355/
- Maurizio Mattoli - https://www.linkedin.com/in/mauriziomattoli/
- Alejandro Ortega

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: 2020.01.10 13:11:57 -03'00'