CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 20 de Marzo de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 12 y el miércoles 18 de Marzo de 2020.

Falsificación de Registro o Identidad

8FFR20-00258-01 CSIRT IDENTIFICÓ PÁGINA BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR20-00258-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Marzo de 2020
Última revisión	12 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/8ffr20-00258-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00258-01.pdf

8FFR20-00259-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00259-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Marzo de 2020
Última revisión	12 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/8ffr20-00259-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00259-01.pdf

8FFR20-00260-01 CSIRT ADVIERTE DE 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00260-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 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 IP que suplantan 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://www.csirt.gob.cl/alertas/8ffr20-00260-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00260-01.pdf

8FFR20-00261-01 CSIRT IDENTIFICÓ 2 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00261-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociado 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/8ffr20-00261-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00261-01.pdf

8FFR20-00262-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00262-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Marzo de 2020
Última revisión	14 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 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/8ffr20-00262-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00262-01.pdf

8FFR20-00263-01 CSIRT IDENTIFICÓ 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00263-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Marzo de 2020
Última revisión	14 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 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/8ffr20-00263-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00263-01.pdf

8FFR20-00264-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00264-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 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/8ffr20-00264-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00264-01.pdf

8FFR20-00265-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00265-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 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/8ffr20-00265-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00265-01.pdf

8FFR20-00266-01 CSIRT ADVIERTE ACTIVACIÓN DE TRES PORTALES FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00266-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 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/8ffr20-00266-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00266-01.pdf

8FFR20-00267-01 CSIRT HA IDENTIFICADO TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00267-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 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://www.csirt.gob.cl/alertas/8ffr20-00267-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00267-01.pdf

8FFR20-00268-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00268-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Marzo de 2020
Última revisión	18 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/8ffr20-00268-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00268-01.pdf

8FFR20-00269-01 CSIRT ADVIERTE ACTIVACIÓN DE CUATRO PORTALES FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00269-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Marzo de 2020
Última revisión	18 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro 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/8ffr20-00269-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00269-01.pdf

8FFR20-00270-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00270-01
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/8ffr20-00270-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00270-01.pdf

Malware

2CMV20-00052-01 CSIRT ADVIERTE MALWARE CON SUPUESTO COMPROBANTE DE PAGO

Alerta de seguridad informática	2CMV20-00052-01
Clase de alerta	Fraude
Tipo de incidente	Malware
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 Servipag.
El mensaje del correo indica que según la información entregada por teléfono, se envía el comprobante por este medio. El atacante persuade para que seleccione el enlace, para así ser dirigido a la descarga de un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión .JS. Al ser ejecutado, se gatilla la descarga el malware.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00052-01/
https://www.csirt.gob.cl/media/2020/03/2CMV20-00052-01.pdf

Phishing

8FPH20-00131-01 CSIRT ADVIERTE PHISHING DE CRÉDITO DE CONSUMO APROBADO

Alerta de seguridad informática	8FPH20-00131-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Marzo de 2020
Última revisión	16 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, indicado que existe un crédito de consumo aprobado y que solo lo puede solicitar a través de la banca en línea. En el correo también se informa que es factible realizar avances de dinero en efectivo con y sin cuotas. El atacante intenta persuadir al usuario que seleccione el enlace para redirigir a la víctima a un sitio semejante al del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00131-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00131-01.pdf

8FPH20-00132-01 CSIRT IDENTIFICÓ PHISHING DE CRÉDITO DE CONSUMO PRE APROBADO

Alerta de seguridad informática	8FPH20-00132-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Marzo de 2020
Última revisión	16 de Marzo de 2020

Resumen

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

El mensaje informa a la víctima sobre un crédito de consumo pre-aprobado con cupo de $4.230.000 millones de pesos. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, 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/8fph20-00132-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00132-01.pdf

8FPH20-00133-01 CSIRT ADVIERTE PHISHING BANCARIO EN PAGO AUTOMÁTICO DE LUZ

Alerta de seguridad informática	8FPH20-00133-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 se encuentra disponible la factura para el pago automático (PAC) de la cuenta de Luz. El mensaje indica que si la persona desea más detalle o cancelar el programa del pago automático, debe acceder directamente a portal de servicios virtual a través del enlace adjunto en el correo. Al seleccionar el enlace indicado, 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/8fph20-00133-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00133-01.pdf

8FPH20-00134-01 CSIRT ADVIERTE PHISHING DE AUMENTO DE TARJETA Y/O LÍNEA DE CRÉDITO

Alerta de seguridad informática	8FPH20-00134-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 de Chile. El mensaje indica que existe un aumento pre aprobado para las Tarjeta y/o Línea de Crédito. El atacante disponibiliza un enlace para que el usuario, al seleccionarlo, sea dirigido a un sitio semejante al del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00134-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00134-01.pdf

8FPH20-00135-01 CSIRT ADVIERTE PHISHING POR MANTENCIÓN DE SERVICIOS

Alerta de seguridad informática	8FPH20-00135-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 de Estado. El mensaje del correo indica que se realizó un mantenimiento en los servicios de Caja Vecina, ServiEstado y Aplicación Web, encontrando un error en su cuenta. Como consecuencia de lo anterior, en el correo de informa a la víctima que se procedió al bloqueo de su cuenta. El atacante disponibiliza un enlace que supuestamente permitiría activar la cuenta bloqueada. Cuando la persona selecciona el enlace, es dirigido a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00135-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00135-01.pdf

8FPH20-00136-01 CSIRT ADVIERTE PHISHING EN ABONOS DE CRÉDITO Y AVANCE

Alerta de seguridad informática	8FPH20-00136-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 de Estado. El mensaje del correo indica que el cliente tiene un crédito de consumo preaprobado y que adicionalmente puede solicitar avances en dinero, ambas acciones con abono inmediato en su cuenta. El atacante disponibiliza un enlace que permitiría supuestamente solicitar el abono, pero al seleccionarlo es dirigido a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00136-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00136-01.pdf

8FPH20-00137-01 CSIRT ADVIERTE DE PHISHING DE SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00137-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Marzo de 2020
Última revisión	17 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 servicio de streaming Netflix. El mensaje del correo indica al cliente sobre la suspensión de su cuenta, razón por la cual debe actualizar su información a través de un enlace dispuestoen el cuerpo del correo. Si una persona intenta utilizar el enlace para actualizar sus datos, es dirigida a un sitio semejante al de Netflix donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00137-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00137-01.pdf

9VSA20-00155-01 CSIRT COMPARTE ACTUALIZACIÓN PARA MOZILLA THUNDERBIRD

Alerta de seguridad informática	9VSA20-00155-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 de Marzo de 2020

Vulnerabilidad

CVE-2020-6805
CVE-2020-6806
CVE-2020-6807
CVE-2020-6811
CVE-2020-6812
CVE-2020-6814
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 Mozilla Thunderbird, 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/9vsa20-00155-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00155-01.pdf

9VSA20-00156-01 CSIRT COMPARTE ACTUALIZACIÓN PARA MICROSOFT

Alerta de seguridad informática	9VSA20-00156-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 de Marzo de 2020

Vulnerabilidad

CVE-2020-0796

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a vulnerabilidad presente en el protocolo SMBv3. Esta vulnerabilidad se comunicó previamente en la alerta 9VSA20-00153-01. Este informe incluye su respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00156-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00156-01.pdf

9VSA20-00157-01 CSIRT COMPARTE ACTUALIZACIÓN DE JOOMLA! PARA SU GESTOR DE CONTENIDOS

Alerta de seguridad informática	9VSA20-00157-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Marzo de 2020
Última revisión	16 de Marzo de 2020

Vulnerabilidad

CVE-2020-10241
CVE-2020-10242
CVE-2020-10238
CVE-2020-10239
CVE-2020-10240
CVE-2020-10243

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Joomla! referente a vulnerabilidades que afectan al gestor de contenidos, las cuales de ser explotadas permitirían a un atacante realizar ataques Cross-site Scripting, Cross-site Request Forgery, inyecciones SQL, entre otros. Este informe incluye su respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00157-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00157-01.pdf

9VSA20-00158-01 CSIRT COMPARTE ACTUALIZACIONES PARA APEXONE, OFFICESCAN Y WORRY-FREE BUSINESS SECURITY

Alerta de seguridad informática	9VSA20-00158-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Marzo de 2020
Última revisión	18 de Marzo de 2020

Vulnerabilidad

CVE-2020-8467
CVE-2020-8468
CVE-2020-8470
CVE-2020-8598
CVE-2020-8599
CVE-2020-8600

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Trend Micro referente a múltiples vulnerabilidades que afectan a los productos Apex One, OfficeScan y Worry-Free Business Security, las cuales de ser explotadas permitirían a un atacante comprometer completamente al sistema afectado. CSIRT hace un llamado a aplicar las medidas de seguridad lo antes posible, pues existen exploits de día 0 explotando estas vulnerabilidades. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00158-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00158-01.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
201.132.92.135	Port Scan
192.241.209.199	Port Scan
69.43.168.245	Malware
87.106.37.146	Malware
210.68.89.106	Port Scan
88.137.132.163	Port Scan
190.188.142.230	Port Scan
103.137.195.120	Port Scan
66.240.205.34	Malware
139.59.70.252	Phishing
142.93.213.201	Phishing
139.59.30.236	Phishing
138.197.173.211	Phishing
178.128.115.229	Phishing
78.140.128.106	Port Scan
62.210.18.16	DDoS
62.210.17.74	DDoS
208.91.197.46	Malware
159.89.175.164	Phishing
157.245.143.176	DDoS
208.123.119.175	Phishing
195.22.26.248	Malware

208.100.26.234	Malware
209.99.40.227	Malware
81.177.143.31	DDoS
220.184.109.62	DDoS
192.33.14.30	Malware
221.222.84.118	DDoS
101.88.193.125	DDoS
112.41.110.160	DDoS
223.155.1.217	DDoS
122.238.26.23	DDoS
120.244.164.79	DDoS
123.115.170.71	DDoS
101.87.4.176	DDoS
122.238.33.83	DDoS
180.111.190.222	DDoS
50.7.146.44	Malware
199.191.50.72	Malware
199.191.50.92	Malware
94.23.64.17	Malware
92.118.37.86	Port Scan
162.243.128.30	Port Scan
182.23.7.194	Port Scan
162.243.129.90	Port Scan
92.118.37.86	Port Scan
41.220.238.138	Port Scan
162.243.130.215	Port Scan
162.243.130.102	Port Scan
1.186.45.162	Port Scan
5.196.198.36	Port Scan
27.72.28.44	Port Scan
13.125.22.61	Port Scan
162.243.129.119	Port Scan
45.227.254.30	Port Scan
46.105.211.42	Port Scan
51.83.217.97	Port Scan
77.247.108.77	Port Scan
94.237.70.143	Port Scan
162.243.132.235	Port Scan
162.213.254.115	Port Scan
162.243.133.125	Port Scan
162.243.128.180	Port Scan

162.243.130.38	Port Scan
162.243.133.172	Port Scan
171.67.70.80	Port Scan
171.67.70.112	Port Scan
162.243.133.187	Port Scan
185.175.93.100	Port Scan
185.176.27.246	Port Scan
192.241.239.53	Port Scan
192.241.237.195	Port Scan
197.163.52.2	Port Scan
197.166.252.2	Port Scan
51.15.21.178	Port Scan
184.105.192.2	Malware
195.22.26.248	Malware
217.12.199.90	Malware
192.241.235.236	Malware
217.61.20.207	Malware
193.142.146.21	Malware
185.176.27.62	Malware
195.154.182.117	Malware
162.243.131.32	Port Scan
162.243.132.5	Port Scan
192.241.238.118	Port Scan
193.187.118.237	Port Scan
54.39.215.32	Port Scan
89.207.236.7	Port Scan
216.104.41.99	Port Scan
68.183.79.125	Port Scan
178.128.47.75	Port Scan
149.28.192.13	Port Scan
139.162.19.101	Port Scan
185.172.110.230	Port Scan
205.204.85.3	Port Scan
162.243.132.150	Port Scan
162.243.132.26	Port Scan
162.243.132.33	Port Scan
192.241.239.73	Port Scan
66.151.211.170	Port Scan
94.102.57.140	Port Scan
162.243.128.245	Port Scan
162.243.129.83	Port Scan

185.53.88.42	Port Scan
207.180.213.210	Port Scan
62.171.158.33	Port Scan
83.97.20.251	Port Scan
45.143.220.99	Port Scan
192.241.237.121	Port Scan
89.248.168.157	Port Scan
89.248.174.3	Port Scan
162.243.132.168	Port Scan
115.214.202.32	DDoS
192.241.237.227	Port Scan
194.26.29.121	Port Scan
162.241.253.120	Phishing
50.7.146.51	Malware
51.38.189.136	Phishing
103.133.105.248	Port Scan
139.162.126.103	Phishing
142.93.223.33	Phishing
162.243.133.88	Port Scan
212.129.17.32	Port Scan
192.241.237.251	Port Scan
192.241.235.179	Port Scan
194.26.29.124	Port Scan
147.75.45.195	Port Scan
194.26.29.122	Port Scan
194.26.29.126	Port Scan
171.67.70.81	Port Scan
162.243.132.93	Port Scan
171.67.70.85	Port Scan
79.124.62.66	Port 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.

- Claudio Pontigo. Linkedin: https://www.linkedin.com/in/clapontigo
- Pablo Cruces Araya. Linkedin: https://www.linkedin.com/in/pablo-cruces-araya-48985112a/

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: 2020.03.20 13:54:19 -03'00'