13BCS-00026-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 24 de Octubre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el miércoles 11 y el jueves 24 de Octubre.

Falsificación de Registro o Identidad

8FFR-00085-001 CSIRT ADVIERTE SOBRE SITIO WEB BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00085-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Octubre de 2019
Última revisión	10 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Scotiabank, lo 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-00085-001/

https://www.csirt.gob.cl/media/2019/10/8FFR-00085-001.pdf

8FFR-00086-001 CSIRT ADVIERTE DE NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00086-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Octubre de 2019
Última revisión	11 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Chile, lo 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-00086-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00086-001.pdf

8FFR-00087-001 CSIRT INFORMA DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00087-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Octubre de 2019
Última revisión	11 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial 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/8ffr-00087-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00087-001.pdf

8FFR-00088-001 CSIRT ADVIERTE DE ACTIVACIÓN DE PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00088-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Octubre de 2019
Última revisión	14 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de 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/8ffr-00089-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00089-001.pdf

8FFR-00089-001 CSIRT INFORMA SOBRE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00089-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Octubre de 2019
Última revisión	14 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Scotiabank, lo 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-00089-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00089-001.pdf

8FFR-00090-001 CSIRT ADVIERTE DE PORTALES FRAUDULENTOS ASOCIADOS A UNA IP QUE SUPLANTAN A 10 BANCOS

Alerta de seguridad informática	8FFR-00090-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Octubre de 2019
Última revisión	15 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de una serie de portales bancarios fraudulentos asociado a una IP que redirige a sitios que suplantan a 10 bancos que operan en Chile, con el propósito de robar credenciales de usuarios de las entidades: Banco Scotiabank; Banco Chile; Banco Estado; Banco Falabella; Banco Bci; Banco Bice; Banco Itau; Banco Santander; Banco Security; y Banco Ripley. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a las entidades bancarias aludidas..

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00090-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00090-001.pdf

8FFR-00091-001 CSIRT ADVIERTE DE WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR-00091-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Octubre de 2019
Última revisión	15 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial 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/8ffr-00091-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00091-001.pdf

8FFR-00092-001 CSIRT ADVIERTE DE ACTIVACIÓN DE 10 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00092-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Octubre de 2019
Última revisión	15 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de una serie de portales bancarios fraudulentos asociado a una IP que redirige a sitios que suplantan a 10 bancos que operan en Chile, con el propósito de robar credenciales de usuarios de las entidades: Banco Scotiabank; Banco Chile; Banco Estado; Banco Falabella; Banco Bci; Banco Bice; Banco Itau; Banco Santander; Banco Security; y Banco Ripley. 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-00092-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00092-001.pdf

8FFR-00093-001 CSIRT ADVIERTE DE SITIOS BANCARIOS FRAUDULENTOS QUE PODRÍAN ROBAR DATOS DE CLIENTES

Alerta de seguridad informática	8FFR-00093-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Octubre de 2019
Última revisión	16 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Estado, lo 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-00093-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00093-001.pdf

8FFR-00094-001 CSIRT ADVIERTE DE ACTIVACIÓN DE PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00094-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Octubre de 2019
Última revisión	17 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial 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/8ffr-00094-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00094-001.pdf

8FFR-00095-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE CREDENCIALES DE CLIENTES BANCARIOS

Alerta de seguridad informática	8FFR-00095-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Octubre de 2019
Última revisión	18 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco BCI, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00095-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00095-001.pdf

8FFR-00096-001 CSIRT ADVIERTE DE UNA SERIE DE SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00096-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Octubre de 2019
Última revisión	18 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco de Chile, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00096-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00096-001.pdf

8FFR-00097-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE credenciales

Alerta de seguridad informática	8FFR-00097-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Octubre de 2019
Última revisión	22 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco de 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/8ffr-00097-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00097-001.pdf

8FPH-00067-001 CSIRT ADVIERTE DE PHISHING EN CORREO QUE ADVIERTE DE FRAUDE EN CUENTA

Alerta de seguridad informática	8FPH-00067-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Octubre de 2019
Última revisión	23 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Chile. El correo indica que se ha detectado una operación fraudulenta la que debe ser suspendida por el propio usuario a través de un enlace que está disponible en el correo. Una vez que ingresan en el enlace quedan expuestos al robo de sus credenciales desde un sitio semejante al del Banco.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00067-001/
https://www.csirt.gob.cl/media/2019/10/8FPH-00067-001.pdf

8FPH-00068-001 CSIRT ADVIERTE SOBRE CAMPAÑA DE PHISHING CON DIFERENTES MENSAJES

Alerta de seguridad informática	8FPH-00068-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Octubre de 2019
Última revisión	23 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Chile. El atacante utiliza varios mensajes en el cuerpo del correo para persuadir al usuario para que seleccione un enlace, siendo direccionado a un sitio semejante al del banco. De esta forma los estafadores podrían capturar las credenciales bancarias de los clientes. A continuación se detallan algunos de los mensajes con los que se intenta engañar a los usuarios: Bloqueo de su tarjeta de débito por una compra sospechosa; Se realizó un descuento porque existió un error; Se realizó una retención por una deuda; Se bloqueó una transacción por ser sospechosa.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00068-001-2/
https://www.csirt.gob.cl/media/2019/10/8FPH-00068-001.pdf

2CMV-00031-002 CSIRT ACTUALIZA INFORMACIÓN DE MALWARE CONTRA CIUDADANÍA Y SISTEMA BANCARIO VÍA USO PROXY CHANGE Y EXTENSIÓN DE CHROME

Alerta de seguridad informática	8FPH-00031-002
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Octubre de 2019
Última revisión	11 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha detectado la activación de la campaña phishing malicioso asociada al script dirigido contra la ciudadanía y el sistema bancario nacional vía uso proxy y extensión de Chrome (JS/ProxyChanger). Esta campaña se identificó a través de correos electrónicos maliciosos, cuyo mensaje intenta suplantar a una empresa de abogados, indicando que ya sé realizo un transferencia a la cuenta del usuario por una compra anulada. El atacante insta al usuario para que imprima el recibo adjunto en el vínculo del correo. Al seleccionar el vínculo se gatilla el proceso de infección, direccionado a la url https://servicionoreply[.]blognetkatay[.]com/recibo/, donde se descarga el archivo "AdbFlash.zip". Posteriormente es direccionado a http://www.hardlopenvoorbeginners[.]com/media/AdbFlash[.]js y como etapa final se descarga el malware en el equipo de la víctima. En seguida, el usuario visualiza un mensaje que indica que la actualización de Flash Player se efectuó exitosamente.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00031-002/
https://www.csirt.gob.cl/media/2019/10/2CMV-00031-002.pdf

2CMV-00035-001 CSIRT ADVIERTE DE MALWARE EN FALSO CORREO DE TESORERÍA

Alerta de seguridad informática	8FPH-00068-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Octubre de 2019
Última revisión	23 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene de la Tesorería General de la Republica. Los criminales buscan engañar a los usuarios advirtiéndoles sobre una supuesta liquidación tributaria impaga. A la potencial víctima se le ofrece la posibilidad de descargar desde un enlace el informe generado por el Servicio de Impuesto Internos. Al seleccionar el hipervínculo se inicia el proceso para la descarga del archivo malicioso. Junto a este informe se adjuntan indicadores de compromiso.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00035-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00035-001.pdf

Vulnerabilidades

9VSA-00066-001 CSIRT COMPARTE ACTUALIZACIONES PARA ITERM2 DE MACOS

Alerta de seguridad informática	9VSA-00066-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	10 de octubre de 2019
Última revisión	10 de octubre de 2019

Vulnerabilidad

CVE-2019-9535

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por diferentes fuentes referente a una vulnerabilidad que afecta a iTerm2, emulador de consola para macOS.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00066-001-2/
https://www.csirt.gob.cl/media/2019/10/9VSA-00066-001.pdf

9VSA-00067-001 CSIRT COMPARTE ACTUALIZACIONES PARA CHROME

Alerta de seguridad informática	9VSA-00060-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de octubre de 2019
Última revisión	15 de octubre de 2019

Vulnerabilidad

CVE-2019-13693
CVE-2019-13694
CVE-2019-13695
CVE-2019-13696
CVE-2019-13697

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google correspondiente a diversas vulnerabilidades que afectan a su navegador Chrome.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00067-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00067-001.pdf

9VSA-00068-001 CSIRT COMPARTE ACTUALIZACIONES PARA SUDO

Alerta de seguridad informática	9VSA-00068-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	16 de octubre de 2019
Última revisión	16 de octubre de 2019

Vulnerabilidad

CVE-2019-14287

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Red Hat, referente a una vulnerabilidad que afecta a SUDO en la mayoría de las distribuciones de Linux, junto a sus respectivas actualizaciones para mitigar los riesgos.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00068-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00068-001.pdf

9VSA-00069-001 CSIRT COMPARTE ACTUALIZACIONES PARA ACROBAT READER

Alerta de seguridad informática	9VSA-00069-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	17 de Octubre de 2019
Última revisión	17 de Octubre de 2019

Vulnerabilidad

CVE-2019-8064 CVE-2019-8184 CVE-2019-8201 CVE-2019-8163 CVE-2019-8185 CVE-2019-8202
CVE-2019-8164 CVE-2019-8189 CVE-2019-8204 CVE-2019-8168 CVE-2019-8190 CVE-2019-8207
CVE-2019-8172 CVE-2019-8193 CVE-2019-8216 CVE-2019-8173 CVE-2019-8194 CVE-2019-8218
CVE-2019-8182 CVE-2019-8198 CVE-2019-8222 CVE-2019-8165 CVE-2019-8171 CVE-2019-8186
CVE-2019-8191 CVE-2019-8199 CVE-2019-8206 CVE-2019-8175 CVE-2019-8192 CVE-2019-8215
CVE-2019-8176 CVE-2019-8203 CVE-2019-8217 CVE-2019-8177 CVE-2019-8208 CVE-2019-8219
CVE-2019-8178 CVE-2019-8209 CVE-2019-8220 CVE-2019-8179 CVE-2019-8210 CVE-2019-8221
CVE-2019-8180 CVE-2019-8211 CVE-2019-8223 CVE-2019-8181 CVE-2019-8212 CVE-2019-8224
CVE-2019-8187 CVE-2019-8213 CVE-2019-8225 CVE-2019-8188 CVE-2019-8214 CVE-2019-8170
CVE-2019-8183 CVE-2019-8197 CVE-2019-8160 CVE-2019-8162 CVE-2019-8226 CVE-2019-8161
CVE-2019-8167 CVE-2019-8169 CVE-2019-8200 CVE-2019-8174 CVE-2019-8195 CVE-2019-8196
CVE-2019-8205

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Adobe correspondiente a diversas vulnerabilidades que afectan a Acrobat Reader.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00069-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00069-001.pdf

9VSA-00070-001 CSIRT COMPARTE ACTUALIZACIONES PARA VMWARE SD-WAN POR VELOCLOUD

Alerta de seguridad informática	9VSA-00070-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	17 de Octubre de 2019
Última revisión	17 de Octubre de 2019

Vulnerabilidad

CVE-2019-5533

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMware, referente a una vulnerabilidad en VMware SD-WAN por VeloCloud en Linux, junto a su respectiva forma de mitigarla.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00070-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00070-001.pdf

9VSA-00071-001 CSIRT COMPARTE ACTUALIZACIONES PARA ORACLE VM VIRTUALBOX

Alerta de seguridad informática	9VSA-00071-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2019
Última revisión	18 de octubre de 2019

Vulnerabilidad

CVE-2019-2926

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Oracle, referente a una vulnerabilidad que afecta a Oracle VM VirtualBox, junto a su respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00071-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00071-001.pdf

9VSA-00072-001 CSIRT COMPARTE ACTUALIZACIONES PARA FORTIMAIL

Alerta de seguridad informática	9VSA-00072-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2019
Última revisión	21 de octubre de 2019

Vulnerabilidad

CVE-2019-15712

CVE-2019-15707

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Fortiguard Labs correspondiente a dos vulnerabilidades que afectan a FortiMail.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00072-001/

https://www.csirt.gob.cl/media/2019/10/9VSA-00072-001.pdf

9VSA-00073-001 CSIRT COMPARTE ACTUALIZACIONES PARA AVIRA

Alerta de seguridad informática	9VSA-00073-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	22 de octubre de 2019
Última revisión	22 de octubre de 2019

Vulnerabilidad

CVE-2019-15712

CVE-2019-15707

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Avira, referente a una vulnerabilidad en su software de actualización, junto a su respectiva forma de mitigarla.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00073-001/

https://www.csirt.gob.cl/media/2019/10/9VSA-00073-001.pdf

Reportes

REPORTE SOBRE ATAQUES CIBERNÉTICOS DURANTE EL FIN DE SEMANA ENTRE EL 19 Y 20 DE OCTUBRE DE 2019

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó tráfico anómalo en la red de conectividad del Estado y en los sitios web de gobierno que visualiza a través de sus plataformas. Esta anomalía fue detectada entre los días sábado 19, domingo 20 y lunes 21 de octubre de 2019. El siguiente documento resume los eventos y ataques ocurridos durante esos días. CSIRT pudo identificar diferentes fuentes de ataques, siendo la gran mayoría internacionales, y otros nacionales. En este último caso, CSIRT pudo confirmar que existió concertación por parte de grupos nacionales para la perpetración de actividad maliciosa.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00024-001/
https://www.csirt.gob.cl/media/2019/10/10CND-00024-001.pdf

Indicadores de Compromisos

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

IP	motivo
194.187.175.68	Port Scan
69.162.126.126	Port Scan
37.49.231.156	Port Scan
159.203.201.41	Port Scan
62.234.92.113	Port Scan
198.108.67.96	Port Scan
78.157.209.34	Port Scan
185.39.11.41	Port Scan
89.248.160.178	Port Scan
185.176.27.94	Port Scan
185.175.93.18	Port Scan
77.40.4.202	Port Scan
51.89.125.75	Port Scan
191.114.52.29	DdoS
80.211.244.140	Port Scan
104.192.0.62	Port Scan
159.203.201.38	Port Scan
13.59.252.119	Port Scan
139.162.235.92	Port Scan
200.28.77.151	DdoS

201.189.20.253	DdoS
200.28.89.224	DdoS
181.203.59.74	DdoS
186.104.70.200	DdoS
181.163.50.170	DdoS
179.8.102.80	DdoS
186.106.58.211	DdoS
129.78.110.128	Port Scan
139.19.117.8	Port Scan
198.108.67.112	Port Scan
198.12.64.90	Port Scan
190.5.48.132	Port Scan
51.38.67.162	Port Scan
133.34.149.5	Port Scan
185.40.13.3	DdoS
31.166.40.210	DdoS
82.196.5.139	DdoS
194.187.175.68	DdoS
187.189.155.205	DdoS
217.61.59.165	DdoS
172.58.235.123	DdoS
201.219.175.159	DdoS
152.231.32.212	DdoS
178.148.27.26	DdoS
179.7.225.94	DdoS
186.84.193.159	DdoS
64.59.96.67	DdoS
157.37.196.149	DdoS
189.217.25.216	DdoS
186.120.90.2	DdoS
200.86.190.183	DdoS
190.20.144.6	DdoS
179.8.55.186	DdoS
190.37.217.223	DdoS
181.46.136.142	DdoS
189.186.234.207	DdoS
186.51.195.107	DdoS
185.176.27.114	DdoS
141.168.65.80	DdoS
181.115.30.153	DdoS
191.88.96.17	DdoS
186.111.153.74	DdoS

186.84.90.190	DdoS
190.159.208.199	DdoS
181.129.217.34	DdoS
80.211.240.4	Port Scan
77.247.110.73	Port Scan
172.105.26.90	Port Scan
172.105.215.250	Port Scan
50.116.42.192	Port Scan
74.207.231.72	Port Scan
69.171.251.134	Port Scan
173.212.248.207	Port Scan
190.92.0.5	Port Scan
138.246.253.21	Port Scan
66.220.156.50	Port Scan
66.220.156.53	Port Scan
192.236.194.154	Port Scan
88.198.139.2	Port Scan
185.40.13.3	Port Scan
222.187.200.229	Port Scan
89.248.169.12	Port Scan
134.209.173.240	Port Scan
190.164.53.171	Port Scan
190.196.60.169	Port Scan
193.201.28.35	Port Scan
190.8.119.74	Port Scan
200.28.77.151	Port Scan
201.189.20.253	Port Scan
200.28.89.224	Port Scan
181.203.59.74	Port Scan
186.104.70.200	Port Scan
181.163.50.170	Port Scan
179.8.102.80	Port Scan
186.106.58.211	Port Scan
159.203.201.96	Port Scan
80.82.48.104	Port Scan
45.136.109.48	Port Scan
159.89.34.120	Port Scan
23.247.118.11	Port Scan
80.82.65.74	Port Scan
77.247.110.162	Port Scan
144.91.76.173	Port Scan
212.60.5.8	Port Scan

92.118.37.70	Port Scan
159.89.34.120	Port Scan
158.69.58.33	Port Scan
186.20.255.188	Port Scan
138.68.0.180	Port Scan
131.255.7.87	Port Scan
185.216.140.252	Port Scan
186.104.157.97	Port Scan
200.83.20.159	Port Scan
190.47.167.118	Port Scan
80.82.78.104	Port Scan
186.104.131.12	Port Scan
200.27.2.65	Port Scan
205.185.124.24	Port Scan
200.83.18.42	Port Scan
68.183.16.183	Port Scan
196.240.255.14	Port Scan
51.38.107.66	Port Scan
66.220.151.250	Port Scan
66.220.151.252	Port Scan
119.225.142.246	Port Scan
45.131.68.37	Port Scan
190.160.0.51	Port Scan
94.142.136.100	Port Scan
129.28.29.30	Port Scan
144.217.7.33	Port Scan
158.69.58.33	Port Scan
179.4.213.97	Port Scan
203.80.136.133	Port Scan
204.12.240.85	Port Scan
159.203.192.250	Port Scan
81.22.45.170	Port Scan
92.118.37.88	Port Scan
185.136.204.36	Port Scan
185.136.204.35	Port Scan
23.228.101.195	Port Scan
185.140.55.94	Port Scan
67.211.209.151	Port Scan
159.203.201.80	Port Scan
144.91.76.173	Port Scan
45.143.221.2	Port Scan
191.115.95.26	Port Scan

201.189.30.172	Port Scan
191.126.99.170	Port Scan
191.115.5.137	Port Scan
191.125.139.13	Port Scan
191.125.139.13	Port Scan
190.22.0.122	Port Scan
186.104.146.24	Port Scan
190.21.123.27	Port Scan
190.21.104.223	Port Scan
190.153.227.203	Port Scan
45.76.0.183	Port Scan
176.32.34.88	Port Scan
172.105.69.121	Port Scan
89.248.178.217	Port Scan
95.217.255.76	Port Scan
173.252.99.240	Port Scan
173.252.92.120	Port Scan
45.119.240.78	Port Scan
200.11.176.52	Port Scan
207.246.84.11	Port Scan
34.201.223.181	DdoS
176.32.34.40	Port Scan
103.117.133.199	Hacking
202.29.52.237	Hacking
195.154.185.213	Port Scan
185.181.103.94	Port Scan
159.203.193.246	Port Scan
42.231.162.212	Port Scan
42.231.162.228	Port Scan
93.150.13.6	Port Scan
42.231.162.216	Port Scan
5.188.86.156	Hacking
193.227.235.8	Port Scan
129.226.77.188	Hacking
186.9.192.62	Port Scan
190.215.47.99	Port Scan
118.24.147.252	Port Scan
103.229.66.72	Port Scan
185.90.116.0	Port Scan
185.90.117.0	Port Scan
185.90.118.0	Port Scan
114.118.1.130	Hacking

141.98.81.178	Hacking
222.240.236.178	Hacking
159.203.201.154	Port Scan
109.248.250.15	Port Scan
106.12.54.131	Port Scan
77.247.110.213	Hacking
120.92.12.108	Hacking
201.245.200.122	Hacking
148.70.56.157	Hacking
116.255.212.248	Hacking
180.153.66.230	Hacking
132.232.75.222	Hacking
36.156.24.29	Hacking
186.90.29.228	Malware
104.131.58.132	Malware
181.135.153.203	Malware
66.249.85.10	DDoS
66.249.85.12	DDoS
66.249.85.13	DDoS
45.148.10.180	Port Scan
49.232.6.247	Port Scan
111.230.237.170	Port Scan
176.32.34.116	Port Scan
193.235.146.104	Port Scan
62.210.83.41	Port Scan
45.133.180.138	Port Scan
51.79.130.164	Port Scan
176.32.34.132	Port Scan
87.98.175.194	Port Scan
62.210.162.185	Port Scan
118.143.11.74	Malware
150.207.137.25	Malware
178.238.117.35	Malware
192.185.145.18	Malware
192.185.50.91	Malware
200.195.200.141	Malware
200.195.200.146	Malware
200.195.200.150	Malware
202.171.240.205	Malware
129.204.69.45	Port Scan
140.116.99.33	Port Scan
37.120.152.218	Port Scan

209.99.64.52	Port Scan
185.153.196.28	Port Scan
45.32.181.48	Malware
208.67.222.222	Port Scan
208.67.220.220	Port Scan
90.182.147.34	Port Scan
82.223.14.245	Hacking
46.101.174.128	Malware
132.232.131.248	Malware
46.105.17.29	Malware
166.62.40.199	Malware
103.237.144.136	Malware
61.164.207.230	Port Scan
77.247.108.111	Port Scan
106.12.138.192	Hacking
51.89.125.121	Port Scan
212.83.129.50	Port Scan
23.245.65.135	Hacking
74.220.219.70	Hacking
185.200.118.58	Port Scan
159.203.201.15	Port Scan
112.29.140.220	Hacking
150.109.43.226	Hacking
162.209.215.34	Hacking
151.1.48.8	Hacking
190.228.29.221	Hacking
118.24.48.113	Hacking
104.143.136.2	Hacking
194.147.34.62	Port Scan
101.99.3.135	Hacking
159.203.201.120	Port Scan
180.180.243.223	Hacking
114.43.161.70	Hacking
94.177.240.159	Port Scan
80.82.78.100	Port Scan
80.82.77.245	Port Scan
185.53.88.92	Port Scan
162.244.80.164	Port Scan
195.154.183.108	Port Scan
185.53.88.86	Port Scan
185.200.118.79	Port Scan
181.143.101.18	Malware

110.36.234.146	Malware
46.101.212.195	Malware
68.183.190.199	Malware
94.183.71.206	Malware
185.100.85.150	Malware
69.195.124.125	Hacking
37.120.152.210	Port Scan
77.247.110.243	Port Scan
193.201.224.82	Port Scan
45.79.199.242	Port Scan
207.180.250.174	Port Scan
114.43.220.132	Hacking
148.66.147.11	Hacking
111.243.40.214	Hacking

URL	Motivo
http[:]//digitales-aumento-cupo.cf/www.bancochile.cl/pshtp7rha6/rxe2j_persona/login_3dq1/index/loginpzkz/	Phishing
http://b3nefici0.info/warra/imagenes/comun2008/banca-en-linea-personas.html	Phishing
https://primisortya1972.blogspot.com.br/	Phishing
https://elemasspen1983.blogspot.cz/	Phishing
https://johnginknewsbar1985.blogspot.ro/	Phishing
https://grinjackpelip1979.blogspot.com.tr/	Phishing
https://raetimani1980.blogspot.ru/	Phishing
https://beupasehigh1970.blogspot.com.ar/	Phishing
https://eresneyna1980.blogspot.al/	Phishing
https://riadeoliano1989.blogspot.al/	Phishing
https://litisara1980.blogspot.tw/	Phishing
https://baifootbsulung1978.blogspot.ca/	Phishing
https://powsvolpacom1989.blogspot.qa/	Phishing
https://dovneydening1978.blogspot.com.tr	Phishing
https://toalinitho1981.blogspot.si/	Phishing
https://tagssurfdetu1980.blogspot.no/	Phishing
https://fattbidofca1980.blogspot.de/	Phishing
https://treatirbouisluc1971.blogspot.com.ee/pdf	Malware
https://bellsyscdn.com	Malware

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

Campaña

El CSIRT quiere promover una campaña para no confundirse con el bombardeo de información falsa que circula en redes sociales. El llamado es, **ANTES DE VIRALIZAR, VERIFICAR**. La información falsa puede generar confusión, llevarnos a tomar decisiones erradas o generar conflictos.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.24 08:37:00 -03'00'