CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 224

semana del 13 al 19 de octubre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

1

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

1

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

176

Las mitigaciones son útiles en productos de Microsoft, Google, Citrix y varios otros proveedores.

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

CSIRT alerta de la activación de un nuevo sitio fraudulento que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01540-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 octubre, 2023
Última revisión	18 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
http://www-bancofalabella.cl.i-mimex[.]com/1697640676/cmr/home/index	
Dirección IP sitio falso	
173.201.185.67	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01540-01/	

2. Malware

CSIRT alerta de campaña de phishing con malware Agent Tesla en falsa cotización	
Alerta de seguridad cibernética	2CMV23-00430-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 octubre, 2023
Última revisión	13 octubre, 2023
Indicadores de compromiso	
SHA256	
e418ac2813daadef8ed238148ab1b1037567e1262713161 57d7955b2ce6fa858	
1e3e163f9796bf7a5bfd120a3fa29cd1ca5487f740e2b669bfb766d74096bcd3	
5afa7469bccc0b7357d39e8a75cba0a52d44b85de2d9c5a78a0e0c12cef03c06	
b67634b988dfb1f43e7ecd30579fe285e1e57740d646f6896b4f6a0d13cfb9dd	
584e458ff9e83bced5806448aa5a1b678002e9c7cc92a48901c2bb48f9bad29b	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/2cmv23-00430-01/	

3. Vulnerabilidades

CSIRT comparte información de vulnerabilidades parchadas por Fortinet en varios de sus productos	
Alerta de seguridad cibernética	9VSA23-00918-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 octubre, 2023
Última revisión	10 octubre, 2023
CVE	
CVE-2023-42791 CVE-2023-41679 CVE-2023-42788 CVE-2023-25607 CVE-2023-41841 CVE-2023-40714	
Fabricante	
Fortinet	
Productos afectados	
FortiSIEM : 6.4.0 a 7.0.0. FortiOS: 7.0.0 a 7.2.4. FortiManager 6.2.0 a 7.4.0 FortiAnalyzer 6.2.0 a 7.4.0 FortiADC 6.0.0 a 7.1.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00918-01/	

CSIRT informa de actualización de seguridad contenida en WordPress 6.3.2	
Alerta de seguridad cibernética	9VSA23-00919-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 octubre, 2023
Última revisión	16 octubre, 2023
CVE	
41 correcciones de errores más 8 de seguridad (no se especifica CVE).	
Fabricante	
Wordpress	
Productos afectados	
No se especifican.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00919-01/	

CSIRT comparte actualizaciones de seguridad de Progress WS_FTP Server	
Alerta de seguridad cibernética	9VSA23-00920-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 octubre, 2023
Última revisión	16 octubre, 2023
CVE	
CVE-2023-42657 CVE-2023-40045 CVE-2023-40047 CVE-2023-40046 CVE-2023-40048 CVE-2022-27665 CVE-2023-40049	
Fabricante	
Progress	
Productos afectados	
WS_FTP Server versiones anteriores a 8.7.4 y 8.8.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00920-01/	

CSIRT informa de nueva vulnerabilidad de día cero que afecta a Cisco IOS XE	
Alerta de seguridad cibernética	9VSA23-00921-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 octubre, 2023
Última revisión	16 octubre, 2023
CVE	
CVE-2023-20198	
Fabricante	
Cisco	
Productos afectados	
Cisco IOS XE Software	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00921-01/	

CSIRT informa de vulnerabilidad crítica en Royal Elementor Addons and Templates	
Alerta de seguridad cibernética	9VSA23-00922-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 octubre, 2023
Última revisión	17 octubre, 2023
CVE	
CVE-2023-5360	
Fabricante	
Wordpress	
Productos afectados	
Royal Elementor Addons and Templates anteriores a la versión 1.3.78.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00922-01/	

CSIRT comparte información de actualizaciones de seguridad incluidas en el Oracle Critical Patch Update Advisory, octubre 2023	
Alerta de seguridad cibernética	9VSA23-00922-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 octubre, 2023
Última revisión	17 octubre, 2023
CVE	
CVE-2019-10086	
CVE-2019-17498	
CVE-2020-11023	
CVE-2020-11988	
CVE-2020-13956	
CVE-2020-36518	
CVE-2020-7760	
CVE-2021-28165	
CVE-2021-36374	
CVE-2021-37136	
CVE-2021-37533	
CVE-2021-37714	
CVE-2021-40690	
CVE-2021-41165	
CVE-2021-41945	
CVE-2021-43045	
CVE-2022-1471	
CVE-2022-23491	
CVE-2022-24329	
CVE-2022-24834	
CVE-2022-24839	
CVE-2022-25147	
CVE-2022-25647	
CVE-2022-26612	

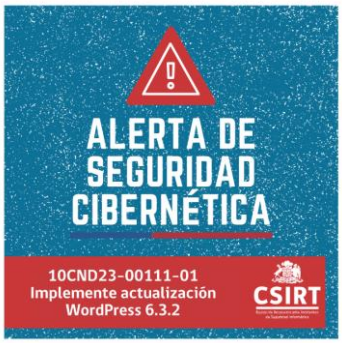
	CVE-2022-29546 CVE-2022-29577 CVE-2022-29599 CVE-2022-31129 CVE-2022-31160 CVE-2022-3171 CVE-2022-33980 CVE-2022-36033 CVE-2022-36944 CVE-2022-37436 CVE-2022-40152 CVE-2022-40982 CVE-2022-41409 CVE-2022-41881 CVE-2022-41954 CVE-2022-41966 CVE-2022-42003 CVE-2022-42004 CVE-2022-42898 CVE-2022-42920 CVE-2022-43680 CVE-2022-44729 CVE-2022-4492 CVE-2022-45061 CVE-2022-45688 CVE-2022-45690 CVE-2022-48285 CVE-2022-4899 CVE-2023-0361 CVE-2023-0568 CVE-2023-1370 CVE-2023-1436 CVE-2023-20862 CVE-2023-20863 CVE-2023-20873 CVE-2023-20883 CVE-2023-21829 CVE-2023-22015 CVE-2023-22019 CVE-2023-22025 CVE-2023-22026 CVE-2023-22028 CVE-2023-22029 CVE-2023-22032 CVE-2023-22043 CVE-2023-22059 CVE-2023-22064 CVE-2023-22065 CVE-2023-22066 CVE-2023-22067 CVE-2023-22068 CVE-2023-22069 CVE-2023-22070 CVE-2023-22071 CVE-2023-22072

	CVE-2023-22073 CVE-2023-22074 CVE-2023-22075 CVE-2023-22076 CVE-2023-22077 CVE-2023-22078 CVE-2023-22079 CVE-2023-22080 CVE-2023-22081 CVE-2023-22082 CVE-2023-22083 CVE-2023-22084 CVE-2023-22085 CVE-2023-22086 CVE-2023-22087 CVE-2023-22088 CVE-2023-22089 CVE-2023-22090 CVE-2023-22091 CVE-2023-22092 CVE-2023-22093 CVE-2023-22094 CVE-2023-22095 CVE-2023-22096 CVE-2023-22097 CVE-2023-22098 CVE-2023-22099 CVE-2023-22100 CVE-2023-22101 CVE-2023-22102 CVE-2023-22103 CVE-2023-22104 CVE-2023-22105 CVE-2023-22106 CVE-2023-22107 CVE-2023-22108 CVE-2023-22109 CVE-2023-22110 CVE-2023-22111 CVE-2023-22112 CVE-2023-22113 CVE-2023-22114 CVE-2023-22115 CVE-2023-22117 CVE-2023-22118 CVE-2023-22119 CVE-2023-22121 CVE-2023-22122 CVE-2023-22123 CVE-2023-22124 CVE-2023-22125 CVE-2023-22126 CVE-2023-22127 CVE-2023-22128 CVE-2023-22129

	CVE-2023-22130 CVE-2023-2283 CVE-2023-22946 CVE-2023-23914 CVE-2023-23931 CVE-2023-24998 CVE-2023-25690 CVE-2023-2603 CVE-2023-26048 CVE-2023-26049 CVE-2023-2650 CVE-2023-26604 CVE-2023-27534 CVE-2023-28439 CVE-2023-28484 CVE-2023-28708 CVE-2023-28709 CVE-2023-29491 CVE-2023-2976 CVE-2023-30535 CVE-2023-30589 CVE-2023-30861 CVE-2023-3247 CVE-2023-33201 CVE-2023-34034 CVE-2023-34396 CVE-2023-34462 CVE-2023-34981 CVE-2023-35116 CVE-2023-35788 CVE-2023-35887 CVE-2023-3635 CVE-2023-38039 CVE-2023-3817 CVE-2023-3824 CVE-2023-38408 CVE-2023-38545 CVE-2023-39017 CVE-2023-39022 CVE-2023-40167 CVE-2023-4039 CVE-2023-41080
	Fabricante
	Oracle
	Productos afectados
	Oracle Analytics Risk Matrix Oracle Banking Branch Oracle Banking Cash Management Oracle Banking Credit Facilities Process Management Oracle Banking Electronic Data Exchange for Corporates Oracle Banking Liquidity Management Oracle Banking Origination Oracle Banking Supply Chain Finance Oracle Banking Trade Finance Process Management Oracle Big Data Spatial and Graph

	Oracle Big Data Spatial and Graph Risk Matrix Oracle Business Intelligence Enterprise Edition Oracle Commerce Risk Matrix Oracle Communications Applications Risk Matrix Oracle Communications Cloud Native Core Policy Oracle Communications Risk Matrix Oracle Construction and Engineering Risk Matrix Oracle Data Integrator Oracle Database Fleet Patching and Provisioning (Apache Mina SSHD) Oracle Database Workload Manager Oracle E-Business Suite products (varios) Oracle E-Business Suite Risk Matrix Oracle Enterprise Manager products (varios) Oracle Enterprise Manager Risk Matrix Oracle Essbase Oracle Essbase Risk Matrix Oracle Financial Services Applications Risk Matrix Oracle Financial Services Cash Flow Engine Oracle Fusion Middleware Risk Matrix Oracle Global Lifecycle Management OPatch Oracle Global Lifecycle Management Risk Matrix Oracle GoldenGate Risk Matrix Oracle GoldenGate Studio Oracle Graph Server and Client Risk Matrix Oracle Health Sciences Applications Risk Matrix Oracle HealthCare Applications Risk Matrix Oracle Hospitality Applications Risk Matrix Oracle Hyperion Risk Matrix Oracle Insurance Applications Risk Matrix Oracle Java SE Risk Matrix Oracle JD Edwards Risk Matrix Oracle MySQL Risk Matrix Oracle PeopleSoft Risk Matrix Oracle REST Data Services Oracle REST Data Services Risk Matrix Oracle Retail Applications Risk Matrix Oracle SD-WAN Edge Oracle Secure Backup Risk Matrix Oracle Siebel CRM Risk Matrix Oracle Spatial and Graph (Google Guava): CVE-2023-2976 [VEX Justification: vulnerable_code_not_in_execute_path]. Oracle Spatial and Graph (SQLite): CVE-2022-46908 [VEX Justification: vulnerable_code_cannot_be_controlled_by_adversary]. Oracle Supply Chain Risk Matrix Oracle Systems Risk Matrix Oracle TimesTen In-Memory Database Risk Matrix Oracle Utilities Applications Risk Matrix Oracle Utilities Network Management System Oracle Virtualization Risk Matrix
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00922-01/

4. Noticias y concientización



Alerta de Seguridad | Llamado a implementar actualización WordPress 6.3.2

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública llama a todos los organismos de la administración pública que utilicen WordPress en alguna de sus páginas web a que implementen la más reciente actualización de mantenimiento y seguridad, WordPress 6.3.2, que incluye ocho parches de seguridad necesarios para evitar exponer su infraestructura tecnológica.

Como siempre, recuerde tomar los debidos resguardos antes de aplicar estas actualizaciones, respaldando sus datos y los del sistema.

Les pedimos también que se preocupen este 7 de noviembre de 2023 de instalar una nueva y más exhaustiva actualización ya anunciada por WordPress, WordPress en su versión 6.4 (https://make.wordpress.org/core/2023/08/22/roadmap-to-6-4/).

Enlaces relevantes:

Version 6.3.2
https://csirt.gob.cl/vulnerabilidades/9vsa23-00918-01/

Asimismo, les recordamos que ante cualquier inquietud sobre esta información u otros requerimientos para detectar y mitigar vulnerabilidades o reportar un incidente, pueden contactar al CSIRT de Gobierno a través del correo electrónico incidentes@interior.gob.cl o llamar al 1510.

Este comunicado también está disponible aquí: https://www.csirt.gob.cl/noticias/10cnd23-00111-01/

10CND23-00112-01 Alerta de seguridad de la información | Ransomware en Aduanas

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública informa a todos los organismos de la administración pública del descubrimiento de un ransomware conocido como Black Basta en una parte acotada de la infraestructura digital del Servicio Nacional de Aduanas.

Por esto, les recomendamos a todos los organismos realizar al menos las siguientes acciones preventivas:

- Verificar que las copias de seguridad se encuentren protegidas y en diferentes lugares.
- Monitorear los Active Directory; se recomienda auditar las cuentas de administración, reducir la cantidad de usuarios con permisos de administración, y chequear los siguientes:
- Creación de cuentas con privilegios
- Elevación de permisos no autorizados
- Aparición de herramientas de escaneos: Netcat – PsExec – PowerShell – Rclone
- Revisar logs de antivirus o sistemas de protección por lo menos 15 días hacia atrás para identificar las amenazas que han sido bloqueadas.
- Revisar qué aplicaciones han sido ejecutadas en los servidores y estaciones de trabajo en el mismo rango de tiempo.
- Forzar un escaneo completo, desactivando la opción de solo analizar archivos nuevos.
- Verificar si existen conexiones a torrents
- Auditar su tráfico de red.
- Conservar un registro actualizado de sus sistemas para garantizar un monitoreo efectivo.
- Revisar la actividad de los eventos de Microsoft Windows (Active Directory) con los siguientes ID:
- Tareas programadas:

    106: El usuario registró una nueva tarea programada
    4702: Se actualizó una tarea programada
    4699: Se eliminó una tarea programada

Servicios

4697: Se instaló un servicio en el sistema
7034: El servicio finalizó inesperadamente
7045: Se creó un nuevo servicio en la máquina local de Windows
Administración de cuentas

4720: Se creó una cuenta de usuario
4724: Se intentó restablecer la contraseña de una cuenta
4782: Acceso a hash de contraseña
4624: Se inició sesión correctamente en una cuenta
4625: Una cuenta no pudo iniciar sesión
4672: Privilegios especiales asignados al nuevo inicio de sesión
4634: Cierre de sesión exitoso
4776: Inicio de sesión fallido o exitoso a través de dominio

Red

5140: Se accedió a un objeto compartido de red
4778: Se volvió a conectar una sesión RDP
4104: Ejecución de PowerShell

Les pedimos asimismo que se mantengan al tanto de esta situación a través de los canales oficiales de información de Aduanas (http://www.aduana.cl/, https://twitter.com/AduanaCL) y del CSIRT (https://www.csirt.gob.cl/noticias, https://twitter.com/CSIRTGOB).

Este comunicado también está disponible aquí: https://www.csirt.gob.cl/noticias/10cnd23-00112-01/

Ciberconsejos | ¿Qué es un phishing con malware?

El phishing es una técnica que busca engañar a las personas, haciéndose pasar por una persona, empresa o servicio de confianza, a través de un correo electrónico, SMS o app de mensajería. Cuando en este correo se adjunta un archivo con malware (programa malicioso), hablamos de phishing con malware. Esta semana en nuestros ciberconsejos te contamos sus características y cómo prevenir.

Revísalo aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-phishing-malware/

5. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

6. 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 del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Fernando González
- Francisco Pinochet
- Francisco Flefil
- Martín Muñoz
- OSI VTI Universidad de Chile
- Milton Reyes
- Felipe Vidal
- Pedro Sandoval
- Andrés Peñalillo

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.20 16:28:02 -03'00'