CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 225

semana del 20 al 25 de octubre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

3

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

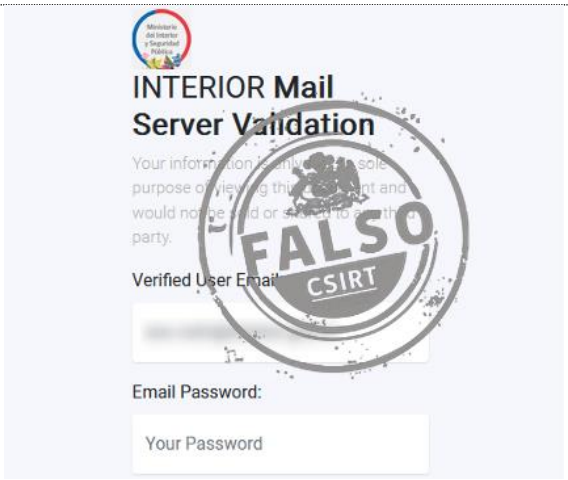
30

Las mitigaciones son útiles en productos de VMware y Juniper Networks.

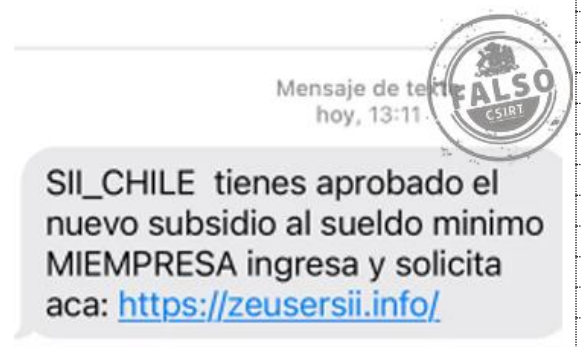
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

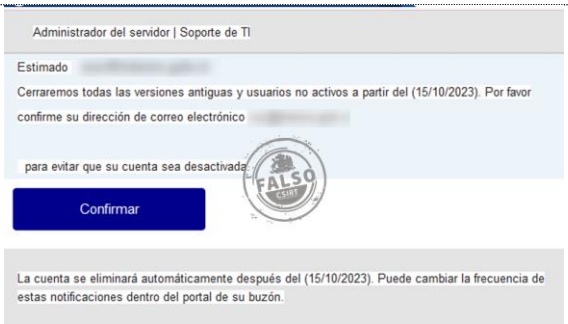
1. Sitios fraudulentos



CSIRT advierte de campaña de phishing con falso aviso de contraseña caducada	
Alerta de seguridad cibernética	8FPH23-00900-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 octubre, 2023
Última revisión	20 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://dev3549.d1tk2ykv7b1ejd.amplifyapp.com/webmails.html#test@csirt.gob.cl	
Dirección IP sitio falso	
[52.84.18.55]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00900-01/	

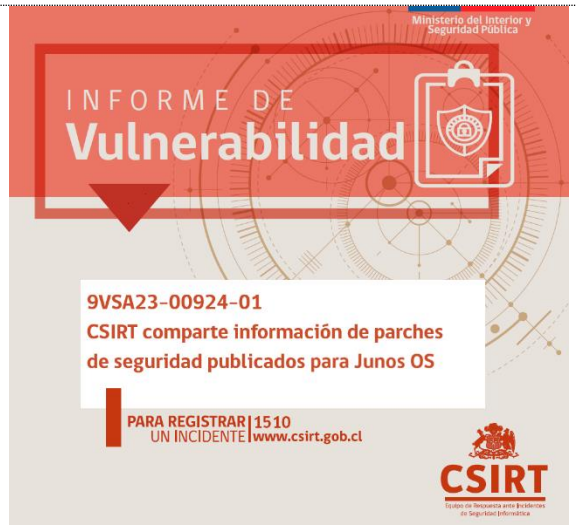


CSIRT alerta de campaña de smishing que suplanta al SII	
Alerta de seguridad cibernética	8FPH23-00901-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 octubre, 2023
Última revisión	23 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://zeusersii[.]info/	
Dirección IP sitio falso	
[172.67.217.33]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00901-01/	

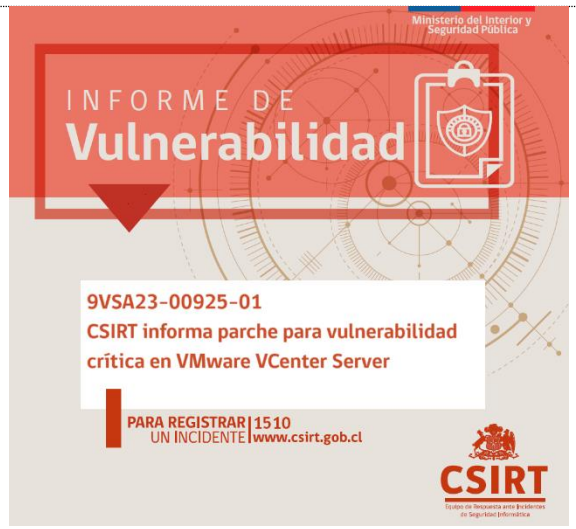


CSIRT informa de nueva campaña de phishing suplantando a Zimbra	
Alerta de seguridad cibernética	8FPH23-00902-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 octubre, 2023
Última revisión	23 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.jimwallermarketing[.]com/1696942336/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[74.125.201.95]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00902-01/	

2. Vulnerabilidades

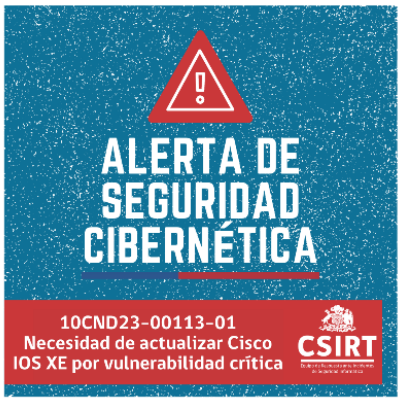


CSIRT comparte de nuevas vulnerabilidades que fueron parchadas para Junos OS		
Alerta de seguridad cibernética	9VSA23-00924-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	24 octubre, 2023	
Última revisión	24 octubre, 2023	
CVE		
CVE-2023-44194	CVE-2023-44196	CVE-2023-44175
CVE-2023-44190	CVE-2023-44195	CVE-2023-36841
CVE-2023-44189	CVE-2023-44187	CVE-2023-36843
CVE-2023-36839	CVE-2023-44201	CVE-2023-44193
CVE-2023-44204	CVE-2023-44199	CVE-2023-44183
CVE-2023-44182	CVE-2023-44188	CVE-2023-44185
CVE-2023-44203	CVE-2023-44191	CVE-2023-44176
CVE-2023-44202	CVE-2023-22392	CVE-2023-44177
CVE-2023-44198	CVE-2023-44192	
CVE-2023-44197	CVE-2023-44178	
Fabricante		
Juniper		
Productos afectados		
Junos OS y Junos OS Evolved		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00924-01/		



CSIRT informa de parche de seguridad ante nueva vulnerabilidad crítica en VMware vCenter Server	
Alerta de seguridad cibernética	9VSA23-00925-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 octubre, 2023
Última revisión	25 octubre, 2023
CVE	
CVE-2023-34048	
CVE-2023-34056	
Fabricante	
VMware	
Productos afectados	
VMware vCenter Server	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00925-01/	

3. Noticias y concientización

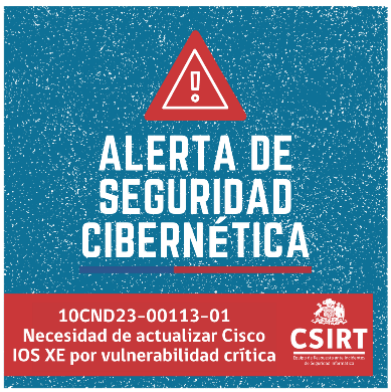


Alerta de seguridad de la información | Explotación de vulnerabilidad en Cisco IOS XE

Compartimos la información dada a conocer por Cisco de la amenaza que supone la explotación activa de la vulnerabilidad CVE-2023-20198, que afecta a su software Cisco IOS XE. Este sistema operativo es fundamental en el funcionamiento de numerosos productos usados por miles de organizaciones en el mundo, incluyendo a Chile.

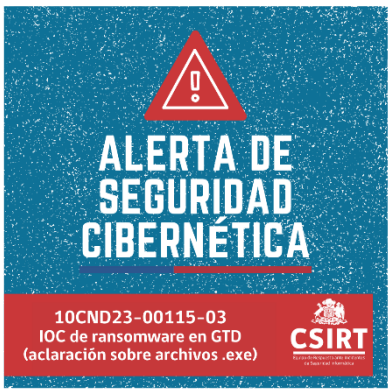
Los detalles: https://csirt.gob.cl/noticias/10cnd23-00113-01/

Alerta de seguridad de la información | Actualización necesaria en Microsoft Exchange Server



Hicimos un llamado a todas las instituciones que utilizan Microsoft Exchange Server a implementar la más reciente actualización de seguridad, liberada el 10 de octubre por Microsoft. Esta actualización incluye la mitigación de una vulnerabilidad crítica identificada como CVE-2023-36778, en la que un atacante autenticado en la misma red que el servidor Exchange puede lograr una ejecución remota de código, a través de una sesión remota de PowerShell.

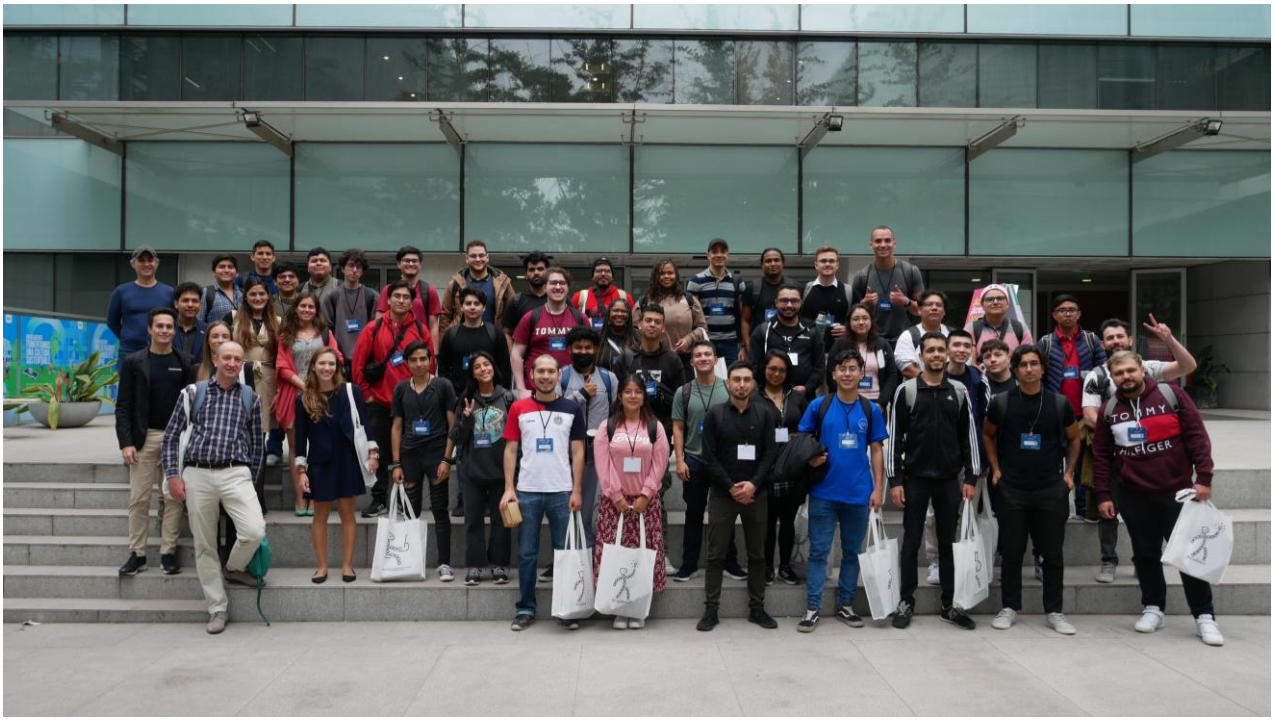
Más información: https://csirt.gob.cl/noticias/10cnd23-00114-01/



Alerta de seguridad de la información | IOC de ransomware en GTD (actualización)

Fuimos informados por la empresa GTD sobre un ransomware que afectó parte de sus plataformas IaaS durante la mañana del lunes 23 de octubreGracias a una muestra compartida por GTD, en el CSIRT hallamos una serie de indicadores de compromiso, los que compartimos en https://csirt.gob.cl/noticias/10cnd23-00115-03/.

Comenzó la final del OEA CyberChallenge con 10 selecciones nacionales compitiendo en nuestro país



Los representantes de Argentina, Brasil, Perú, Guatemala, México, Colombia, Panamá, Costa Rica, República Dominicana y Chile comenzaron este miércoles la definición del equipo nacional ganador del primer OEA CyberChallenge. Esta competencia premia a los jóvenes que mejor se desempeñen en competencias del tipo *Capture de Flag (CTF)*.

Esta final tiene lugar durante mi en el Departamento de Ciencias de la Computación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, a quienes agradecemos su invaluable ayuda para hacer posible esta competencia en nuestro país.

4. 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.26 19:10:13 -03'00'