CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 231

semana del 1 al 6 de diciembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

7

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

103

Las mitigaciones son útiles en productos de Google y Zyxel.

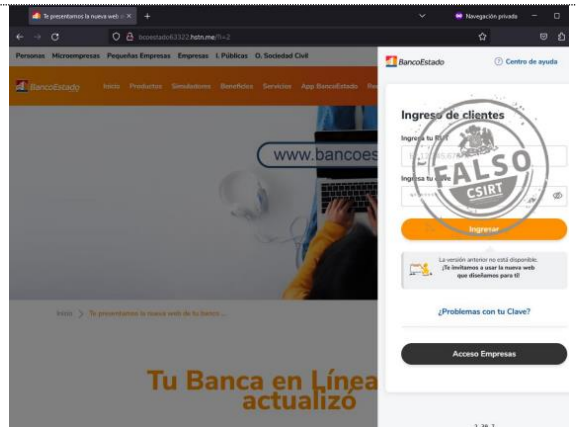
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

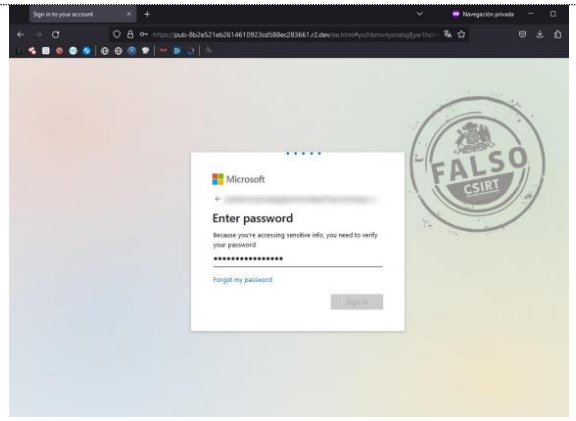
1. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta a empresa contratista del sector minero	
Alerta de seguridad cibernética	8FPH23-00912-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 diciembre, 2023
Última revisión	1 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://ms-onlinesupport[.]com/165959/common/oauth2.0/login/84633/	
Dirección IP sitio falso	
[104.21.11.92]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00912-01/	

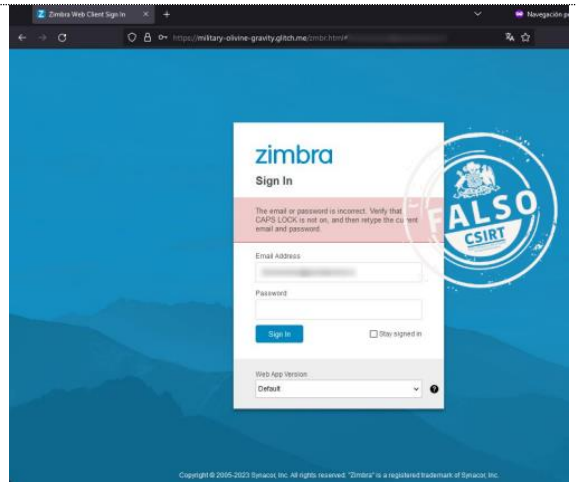
2. Sitios fraudulentos



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01590-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 diciembre, 2023
Última revisión	5 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
http://bcoestado63322.hstn[.]me/?i=2	
URL de redirección	
https://new.express.adobe[.]com/webpage/ZRSKzlMNn4E05	
Dirección IP sitio falso	
[185.27.134.206]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01590-01/	



CSIRT alerta de sitio que suplanta inicio de sesión de Microsoft	
Alerta de seguridad cibernética	8FFR23-01591-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 diciembre, 2023
Última revisión	5 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://pub-8b2e521eb2614610923cd588ec283661.r2.dev/ee.html#yxzhbmvnyxnabgfjyw1hcmfkzxf1axrvlmnvbq==	
URL de redirección	
https://jmgac[.]cl/fo/fo1/172.27.184.69/yxzhbmvnyxnabgfjyw1hcmfkzxf1axrvlmnvbq==?src=insideemail-ironplanet-072523&utm_source=pet&utm_medium=email&utm_campaign=ip-mpe-072523	
Dirección IP sitio falso	
[104.18.3.35]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01591-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta inicio de sesión de Zimbra	
Alerta de seguridad cibernética	8FFR23-01592-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 diciembre, 2023
Última revisión	6 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://alsafua[.]com/red.html#	
URL de redirección	
https://military-olivine-gravity.glitch.me/zmbr.html#	
Dirección IP sitio falso	
[54.84.157.136]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01592-01/	

3. Vulnerabilidades

CSIRT comparte información de nuevas vulnerabilidades que afectan a dispositivos Zyxel NAS	
Alerta de seguridad cibernética	9VSA23-00939-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 diciembre, 2023
Última revisión	1 diciembre, 2023
CVE	
CVE-2023-35137 CVE-2023-35138 CVE-2023-37927 CVE-2023-37928 CVE-2023-4473 CVE-2023-4474	
Fabricante	
Zyxel	
Productos afectados	
NAS326, versiones V5.21(AAZF.14)C0 y anteriores. NAS542, versiones V5.21(ABAG.11)C0 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00939-01/	

CSIRT comparte información de parches en actualización de seguridad de Android para diciembre 2023	
Alerta de seguridad cibernética	9VSA23-00940-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 diciembre, 2023
Última revisión	6 diciembre, 2023

CVE

CVE-2023-33063	CVE-2023-40083	CVE-2022-48457
CVE-2023-33107	CVE-2023-40098	CVE-2022-48458
CVE-2023-33106	CVE-2023-45781	CVE-2022-48459
CVE-2023-40077	CVE-2023-45866	CVE-2023-28588
CVE-2023-40076	CVE-2023-3889	CVE-2023-33053
CVE-2023-40079	CVE-2023-4272	CVE-2023-33063
CVE-2023-40089	CVE-2023-32804	CVE-2023-33079
CVE-2023-40091	CVE-2023-21162	CVE-2023-33087
CVE-2023-40094	CVE-2023-21163	CVE-2023-33092
CVE-2023-40095	CVE-2023-21164	CVE-2023-33106
CVE-2023-40096	CVE-2023-21166	CVE-2023-33107
CVE-2023-40103	CVE-2023-21215	CVE-2022-22076
CVE-2023-45774	CVE-2023-21216	CVE-2022-40507
CVE-2023-45777	CVE-2023-21217	CVE-2023-21652
CVE-2023-21267	CVE-2023-21218	CVE-2023-21662
CVE-2023-40073	CVE-2023-21228	CVE-2023-21664
CVE-2023-40081	CVE-2023-21263	CVE-2023-28546
CVE-2023-40092	CVE-2023-21401	CVE-2023-28550
CVE-2023-40074	CVE-2023-21402	CVE-2023-28551
CVE-2023-40075	CVE-2023-21403	CVE-2023-28586
CVE-2023-40088	CVE-2023-35690	CVE-2023-28585
CVE-2023-40078	CVE-2023-21227	CVE-2023-28587
CVE-2023-40080	CVE-2023-32818	CVE-2023-33017
CVE-2023-40082	CVE-2023-32847	CVE-2023-33018
CVE-2023-40084	CVE-2023-32848	CVE-2023-33022
CVE-2023-40087	CVE-2023-32850	CVE-2023-33054
CVE-2023-40090	CVE-2023-32851	CVE-2023-33080
CVE-2023-40097	CVE-2023-45779	CVE-2023-33081
CVE-2023-45773	CVE-2022-48456	CVE-2023-33088
CVE-2023-45775	CVE-2022-48461	CVE-2023-33089
CVE-2023-45776	CVE-2022-48454	CVE-2023-33097
CVE-2023-21394	CVE-2022-48455	CVE-2023-33098
CVE-2023-35668		

Fabricante

Google

Productos afectados

Android 14 y anteriores.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00940-01/

4. Noticias y concientización

Ciberconsejos | ¿Compras online en Navidad?

Creamos un nuevo video que resume las principales recomendaciones a seguir para comprar de forma más segura en línea, el que está disponible en:https://www.csirt.gob.cl/recomendaciones/ciberconsejos-navidad-2/.

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.

- Bryan Santibáñez SQL Injection
- Christian Campodónico Phishing
- Francisco Flefil Phishing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.12.07 14:57:59 -03'00'