CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 210

semana del 7 al 13 de julio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

9

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

15

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

167

Las mitigaciones son útiles en productos de SAP, Citrix, Microsoft y Mozilla

HASH REPORTADOS

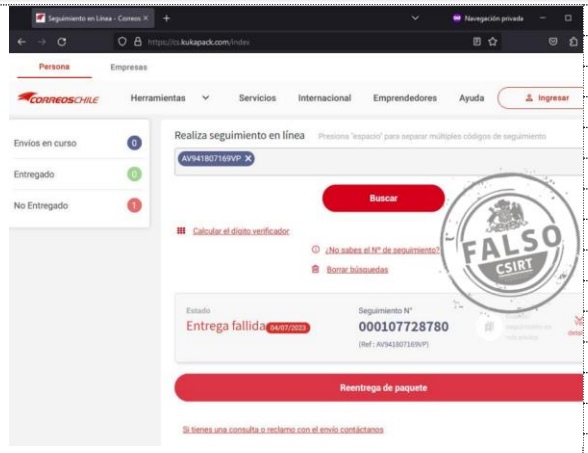
6

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware

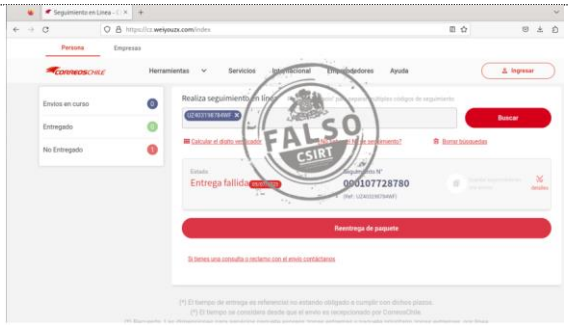
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

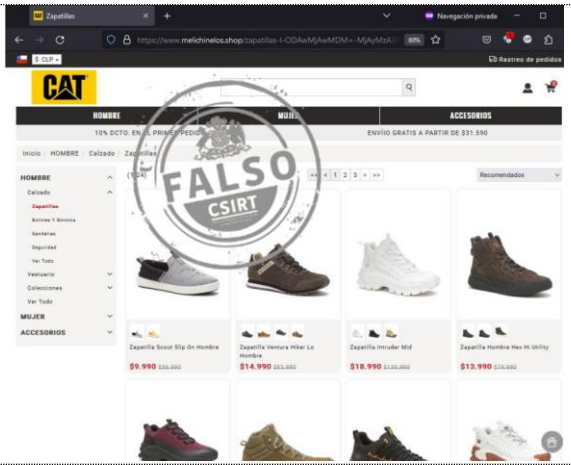
1. Sitios fraudulentos



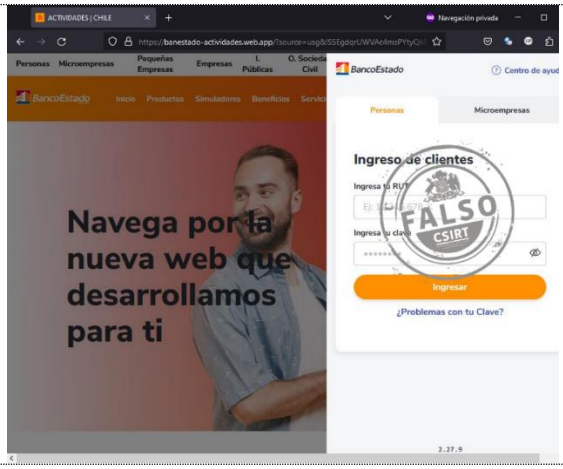
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01457-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 julio, 2023
Última revisión	7 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://cs.kukapack[.]com/index	
Dirección IP	
[43.135.159.200]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01457-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01458-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 julio, 2023
Última revisión	7 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://cz.weiyouzx[.]com/index	
Dirección IP	
[49.51.192.15]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01458-01/	



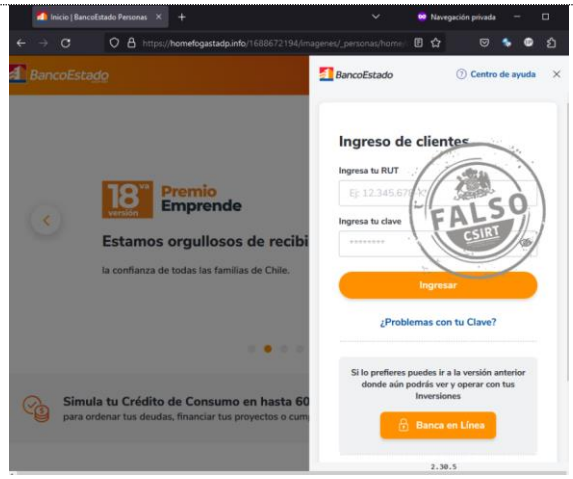
CSIRT alerta ante nuevo sitio fraudulento que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01459-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 julio, 2023
Última revisión	13 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.melichinelos[.]shop	
Dirección IP	
[107.150.173.210]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01459-01/	



CSIRT alerta ante nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01460-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 julio, 2023
Última revisión	13 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://banestado-actividades.web[.]app/	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01460-01/	

2. Phishing

CSIRT alerta de nueva campaña de phishing, que se difunde con falsa actualización de cuenta de email	
Alerta de seguridad cibernética	8FPH23-00853-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 julio, 2023
Última revisión	7 julio, 2023
URL sitio falso	
https://webcenitravencia.wapka[.]co/	
Dirección IP	
[173.212.225.42]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00853-01/	



CSIRT alerta de nueva campaña de phishing, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00854-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 julio, 2023
Última revisión	7 julio, 2023
Indicadores de compromiso	
URL redirección	
https://www.unik[.]mx/activacion/cuenta-bpib/	
URL sitio falso	
https://homefogastadp[.]info/1688672194/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00854-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00855-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 julio, 2023
Última revisión	10 julio, 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-zksc/	
URL sitio falso	
https://fogapepatito[.]com/1688998098/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00855-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing que suplanta al Ministerio de Transportes	
Alerta de seguridad cibernética	2CMV23-00423-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 julio, 2023
Última revisión	12 julio, 2023
Indicadores de compromiso	
URL-Dominio	
https://p-tekng.com/wp-content/themes/–/NEX/dasssashytsrfwewdw4w432dcadssswe32dsfwywyw67wjjehnsbvcdfreyd.php	
SHA256	
bc5b31facbded74c5fd435198a28ffad8e9191bcb7af3fccd6671de3849e08afbe77fceb122776f894dea1a78d076cf4e667044a9fcadf781a613a4bc93d16ee	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00423-01/	

CSIRT alerta de nueva campaña de phishing con malware, que suplanta al SII	
Alerta de seguridad cibernética	2CMV23-00424-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 julio, 2023
Última revisión	13 julio, 2023
Indicadores de compromiso	
URL-Dominio	
https://khojney[.]com/wp-content/plugins/–/factura/ 34.210.155[.]57:9995 mobilforstarkare@65-108-78-58.cprapid.com dh_isqdy3@richard-stockton.dreamhost.com	
SHA256	
0ffc01fec8cc27af51fa6796db3225562d40f92008ea0877f28876a91b4357f40c2094a3608e9f3fe6a874a61097137c8118671a79b25e2a5b989c5cabbfe89b	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00424-01/	


PDI Virtual - Solicitamos su presencia ante el tribunal de justicia.

PDI VIRTUAL <proceso_de_denuncia13594@pdichile.cl>

Responder | Responder a todos | Reenviar

PDI

ÓRDEN DE CITACIÓN

Documentos Requeridos para Audiencia por Citación 2023

CSIRT alerta ante nueva campaña de phishing con malware, que suplanta a la PDI	
Alerta de seguridad cibernética	2CMV23-00425-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 julio, 2023
Última revisión	13 julio, 2023
Indicadores de compromiso	
URL-Dominio	
https://www.elo.net[.]br/wp-content/languages/pdi/dasssashytsrfwewdw4w432dcadssswe32dsfwywyw67wjjehnsbvcdfreyd.php http://servers.itresources[.]am/itr/public/teams/ mobilforstarkare@65-108-78-58[.]cprapid.com	
SHA256	
462a814f8b26279cfc71dbdf874d7c9c626f61811516d5705da9eb0dd32e441b969c4d790314beca402ba8cc253ceb9af856c1ed22aae512e245a9538ea86b95	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00425-01/	

4. Vulnerabilidades

CSIRT comparte información de parches para vulnerabilidades en Firefox 115		
Alerta de seguridad cibernética	9VSA23-00858-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 julio, 2023	
Última revisión	11 julio, 2023	
CVE		
CVE-2023-37201	CVE-2023-37207	CVE-2023-37212
CVE-2023-37202	CVE-2023-37208	CVE-2023-37455
CVE-2023-37203	CVE-2023-37209	CVE-2023-37456
CVE-2023-37204	CVE-2023-37210	CVE-2023-3600
CVE-2023-37205	CVE-2023-37211	CVE-2023-3482
CVE-2023-37206		
Fabricante		
Mozilla		
Productos afectados		
Firefox 115, Firefox for iOS 115, Firefox ESR 115 y Thunderbird 102.13.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00858-01/		

CSIRT comparte vulnerabilidades incluidas en el Update Tuesday de Microsoft para julio 2023		
Alerta de seguridad cibernética	9VSA23-00859-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 julio, 2023	
Última revisión	11 julio, 2023	
CVE		
CVE-2023-21526	CVE-2023-33161	CVE-2023-35328
CVE-2023-21756	CVE-2023-33162	CVE-2023-35329
CVE-2023-29347	CVE-2023-33163	CVE-2023-35330
CVE-2023-32033	CVE-2023-33164	CVE-2023-35331
CVE-2023-32034	CVE-2023-33165	CVE-2023-35332
CVE-2023-32035	CVE-2023-33166	CVE-2023-35333
CVE-2023-32037	CVE-2023-33167	CVE-2023-35335
CVE-2023-32038	CVE-2023-33168	CVE-2023-35336
CVE-2023-32039	CVE-2023-33169	CVE-2023-35337
CVE-2023-32040	CVE-2023-33170	CVE-2023-35338
CVE-2023-32041	CVE-2023-33171	CVE-2023-35339
CVE-2023-32042	CVE-2023-33172	CVE-2023-35340
CVE-2023-32043	CVE-2023-33173	CVE-2023-35341
CVE-2023-32044	CVE-2023-33174	CVE-2023-35342
CVE-2023-32045	CVE-2023-35296	CVE-2023-35343
CVE-2023-32046	CVE-2023-35297	CVE-2023-35344
CVE-2023-32047	CVE-2023-35298	CVE-2023-35345
CVE-2023-32049	CVE-2023-35299	CVE-2023-35346
CVE-2023-32050	CVE-2023-35300	CVE-2023-35347

CVE-2023-32051	CVE-2023-35302	CVE-2023-35348
CVE-2023-32052	CVE-2023-35303	CVE-2023-35350
CVE-2023-32053	CVE-2023-35304	CVE-2023-35351
CVE-2023-32054	CVE-2023-35305	CVE-2023-35352
CVE-2023-32055	CVE-2023-35306	CVE-2023-35353
CVE-2023-32056	CVE-2023-35308	CVE-2023-35356
CVE-2023-32057	CVE-2023-35309	CVE-2023-35357
CVE-2023-32083	CVE-2023-35310	CVE-2023-35358
CVE-2023-32084	CVE-2023-35311	CVE-2023-35360
CVE-2023-32085	CVE-2023-35312	CVE-2023-35361
CVE-2023-33127	CVE-2023-35313	CVE-2023-35362
CVE-2023-33134	CVE-2023-35314	CVE-2023-35363
CVE-2023-33148	CVE-2023-35315	CVE-2023-35364
CVE-2023-33149	CVE-2023-35316	CVE-2023-35365
CVE-2023-33150	CVE-2023-35317	CVE-2023-35366
CVE-2023-33151	CVE-2023-35318	CVE-2023-35367
CVE-2023-33152	CVE-2023-35319	CVE-2023-35373
CVE-2023-33153	CVE-2023-35320	CVE-2023-35374
CVE-2023-33154	CVE-2023-35321	CVE-2023-36867
CVE-2023-33155	CVE-2023-35322	CVE-2023-36868
CVE-2023-33156	CVE-2023-35323	CVE-2023-36871
CVE-2023-33157	CVE-2023-35324	CVE-2023-36872
CVE-2023-33158	CVE-2023-35325	CVE-2023-36874
CVE-2023-33159	CVE-2023-35326	CVE-2023-3688
CVE-2023-33160		

Fabricante

Microsoft

Productos afectados

.NET 6.0
Azure Service Fabric 9.1 for Windows
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Malware Protection Engine
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office for Universal
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Outlook 2016 (32-bit edition)
Microsoft Power Apps (online)
Microsoft SharePoint Server Subscription Edition
Microsoft Visual Studio 2022 version 17.0
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Mono 6.12.0
Paint 3D
PandocUpload
Raw Image Extension
Visual Studio Code – GitHub Pull Requests and Issues Extension
VP9 Video Extensions
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems

	Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows Admin Center Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 (Server Core installation) Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00859-01/

CSIRT comparte información de nuevas vulnerabilidades parchadas por Fortinet para FortiOS y FortiProxy	
Alerta de seguridad cibernética	9VSA23-00860-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 julio, 2023
Última revisión	12 julio, 2023
CVE	
CVE-2023-33308 CVE-2023-33306	CVE-2023-28001 CVE-2023-27997
Fabricante	
Fortinet	
Productos afectados	
FortiOS-6K7K 7.0.5 a 6.0.10. FortiOS: 7.2.4 a 6.0.0. FortiProxy 7.2.3 a 1.1.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00860-01/	

CSIRT comparte información de nueva vulnerabilidad parchada en Citrix Secure Access para Ubuntu	
Alerta de seguridad cibernética	9VSA23-00861-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 julio, 2023
Última revisión	12 julio, 2023
CVE	
CVE-2023-24492	
Fabricante	
Citrix	
Productos afectados	
Citrix Secure Access client for Ubuntu (previously Citrix Gateway VPN client for Ubuntu), versiones anteriores a la 23.5.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00861-01/	

CSIRT informa vulnerabilidades parchadas por SAP en su SAP Security Patch Day de Julio 2023		
Alerta de seguridad cibernética	9VSA23-00862-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	12 julio, 2023	
Última revisión	12 julio, 2023	
CVE		
CVE-2023-36922	CVE-2023-36921	CVE-2023-36919
CVE-2023-33989	CVE-2023-35873	CVE-2023-35874
CVE-2023-33987	CVE-2023-35872	CVE-2023-36917
CVE-2023-33991	CVE-2023-35870	CVE-2023-31405
CVE-2023-33990	CVE-2023-33988	CVE-2023-36924
CVE-2023-35871	CVE-2023-36918	CVE-2023-33992
CVE-2023-36925	CVE-2023-36920	
Fabricante		
SAP		
Productos afectados		
SAP ECC and SAP S/4HANA (IS-OIL) versiones 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807. SAP Business Client, Versions -6.5, 7.0, 7.70. SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757 SAP UI5 Variant Management, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200. SAP SQL Anywhere, Version-17.0. SAP Solution Manager (Diagnostic Agent), Versions –7.20. SAP NetWeaver Process Integration (Runtime Workbench), Versions–SAP_XITOOL 7.50. SAP NetWeaver Process Integration (Message Display Tool), Versions–SAP_XIAF 7.50. SAP NetWeaver AS ABAP and ABAP Platform, Version -KRNL64NUC7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53,		

	KERNEL 7.22, KERNEL7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93. SAP BusinessObjects BI Platform (Enterprise),Version -4.20, 430. SAP NetWeaver AS for Java (Log Viewer), Version -ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50. SAP ERP Defense Forces and Public Security, Version -600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807. SAP Business Warehouseand SAP BW/4HANA, Version -SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300. SAP Web Dispatcher, Versions–WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1 SAP S/4HANA (Manage Journal Entry Template), Versions–S4CORE 104, 105, 106, 107. SAP Enable Now, Version -WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704.
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00862-01/

5. Concientización

Ciberconsejos para evitar ser víctima del vishing

El vishing es una forma de estafa tipo phishing, que se realiza de forma telefónica o por audios a través de plataformas de mensajería, con el objetivo de robar información personal y confidencial de las víctimas, como números de tarjetas bancarias, obtener contraseñas y datos de identificación. ¿Cómo identificar este tipo de fraude y cómo impedir que caigamos en él? Te lo contamos aquí, en la siguientes imágenes que también pueden ser descargadas en: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-vishing/.

6. 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.

7. 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.

- Jorge Ignacio Molina Martínez
- Cristóbal Ramón Herrera Jara
- Gersom Lara
- Rodrigo Zamora Nelson
- Camila Francisca Hevia Salgado
- Sugy Nam
- Juan Velasco
- Javier Andrés Godoy Hernández
- Luis Egaña Valle
- Mario Andrés Faúndez Morales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.21 12:14:53 -04'00'