CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 184

SEMANA DEL 6 AL 12 de enero

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

160

Las mitigaciones son útiles en productos de Jsonwebtoken, Microsoft, Adobe, Intel, SAP, Cisco, Cacti, Avast, AVG, Avira y Norton.

IP INFORMADAS

28

Listado de IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

24

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

4

Asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

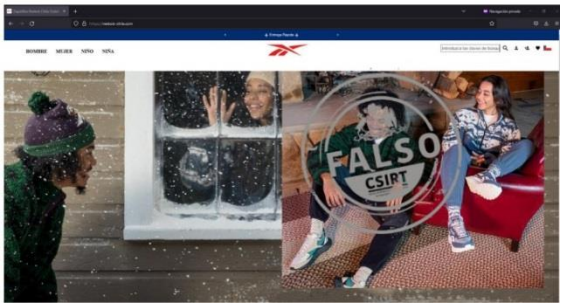
Imagen del sitio		
	**CSIRT alerta de sitio fraudulento que suplanta a Zimbra**	
	Alerta de seguridad cibernética	8FFR23-01191-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	9 de enero de 2023
	Última revisión	9 de enero de 2023
	Indicadores de compromiso	
	URL sitio falso	
	https[:]//cark[.]cl/wp-includes/zim/today/zimbra/	
	Dirección IP	
	[190.13.188.108]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr23-01191-01/	
	https://www.csirt.gob.cl/media/2023/01/8FFR23-01191-01.pdf	

Imagen del sitio		
	**CSIRT alerta de una página fraudulenta que suplanta a Nike**	
	Alerta de seguridad cibernética	8FFR23-01192-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de enero de 2023
	Última revisión	10 de enero de 2023
	Indicadores de compromiso	
	URL sitio falso	
	https[:]//www.nikechile[.]com/	
	Dirección IP	
	[196.196.13.198]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01193-01/	
	https://www.csirt.gob.cl/media/2023/01/8FFR23-01192-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta a sandalias Teva	
Alerta de seguridad cibernética	8FFR23-01193-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//teva-chile[.]com/	
Dirección IP	
[104.21.39.107]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01193-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01193-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta a Reebok	
Alerta de seguridad cibernética	8FFR23-01194-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//reebok-chile[.]com/	
Dirección IP	
[165.231.154.138]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01194-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01194-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta a Adidas	
Alerta de seguridad cibernética	8FFR23-01195-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//tiendaadidaschile[.]com/	
Dirección IP	
[196.196.204.20]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01195-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01195-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta a ABCDin	
Alerta de seguridad cibernética	8FFR23-01196-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//descuento-cl.myshopify[.]com/	
Dirección IP	
[23.227.38.74]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01196-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01196-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que simula ser un sitio de ventas online	
Alerta de seguridad cibernética	8FFR23-01197-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//dorkvl[.]com/	
Dirección IP	
[104.17.232.29]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01197-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01197-01.pdf	

2. Phishing

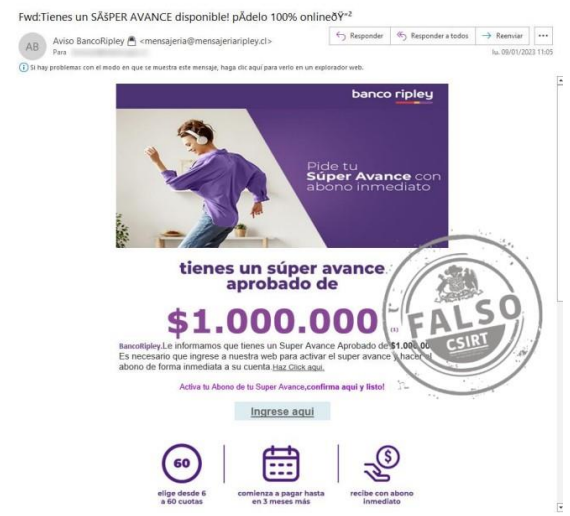
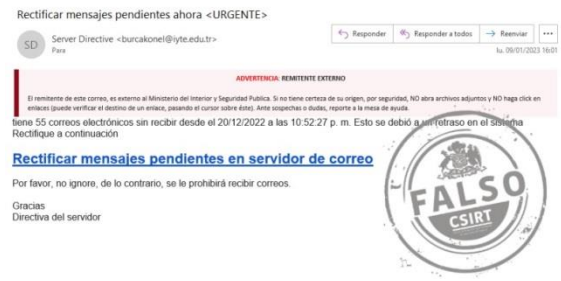
Imagen del mensaje		
	CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
	Alerta de seguridad cibernética	8FPH23-00704-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	9 de enero de 2023
	Última revisión	9 de enero de 2023
	Indicadores de compromiso	
	URL redirección	
	https[:]//bit[.]ly/3WXEYn5?l=www.bancoripley.cl	
	https[:]//sam-tech[.]jp/bancoripley/cuenta-cugb/	
	URL sitio falso	
	https[:]//web-bancoripley-cl.wonthaggicaravans.com[.]au/1673290008/login	
	Dirección IP	
	[203.26.41.136]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00704-01/	
	https://www.csirt.gob.cl/media/2023/01/8FPH23-00704-01.pdf	

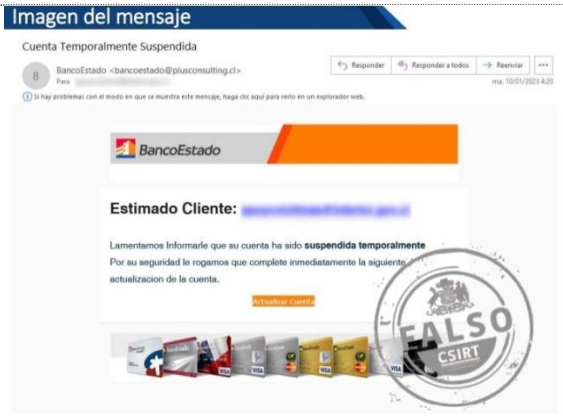
Imagen del mensaje		
	CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
	Alerta de seguridad cibernética	8FPH23-00705-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	9 de enero de 2023
	Última revisión	9 de enero de 2023
	Indicadores de compromiso	
	URL redirección	
	https[:]//ucmstudio[.]info/activacion/cuenta-qvqk/	
	URL sitio falso	
	https[:]//nhmwcotitostado[.]info/1673290679/imagenes/_personas/home/default.asp	
	Dirección IP	
	[172.67.156.230]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00705-01/	
	https://www.csirt.gob.cl/media/2023/01/8FPH23-00705-01.pdf	

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH23-00706-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//firebasestorage.googleapis[.]com/v0/b/uuieywueuriw.appspot.com/o/index.html?alt=media&token=0f3dc7fa-f323-4696-bab9-65769b53f723	
Dirección IP	
[108.177.120.95]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00706-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00706-01.pdf	

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00707-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//xtraillconver[.]com/activacion/cuenta-vtqz/	
URL sitio falso	
https[:]//springpatito[.]info/1673352699/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.10.152]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00707-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00707-01.pdf	

Imagen del mensaje

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00708-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//ucmstudio[.]info/activacion/cuenta-qvqk/	
URL sitio redirección	
https[:]//nhmwcotitostado[.]info/1673356659/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.156.230]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00708-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00708-01.pdf	

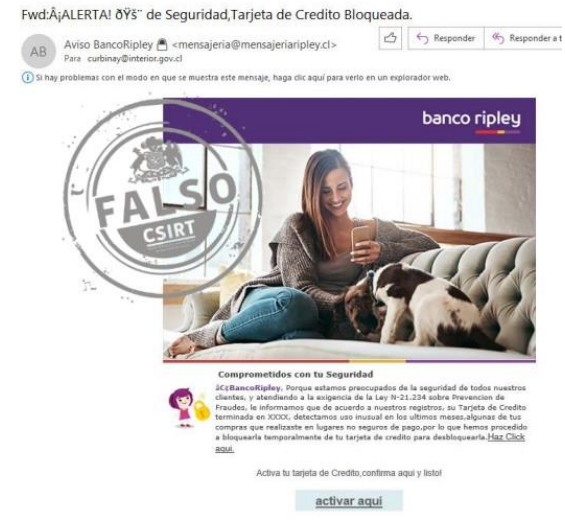
Imagen del mensaje

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00709-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//xtraillconver[.]com/activacion/cuenta-vtqz/	
URL sitio falso	
https[:]//springpatito[.]info/1673440791/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.10.152]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00709-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00709-01.pdf	

Imagen del mensaje

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00710-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//xtraillconver[.]com/activacion/cuenta-hedd/	
URL sitio falso	
https[:]//springpatito[.]info/1673443003/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.163.158]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00710-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00710-01.pdf	

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00711-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3k85YBR?l=www.bancoripley.cl	
https[:]//sam-tech[.]jp/bancoripley/cuenta-qiec/	
URL sitio falso	
https[:]//web-bancoripley-cl.awadgallery.co[.]uk/1673526041/login	
Dirección IP	
[23.88.71.133]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00711-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00711-01.pdf	

3. Malware

Imagen del mensaje		
	**CSIRT alerta de campaña de phishing con malware, que suplanta a Agrical**	
	Alerta de seguridad cibernética	2CMV23-00395-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	11 de enero de 2023
	Última revisión	11 de enero de 2023
	Indicadores de compromiso	
	Asunto	
	RES: Ref: viejo orden_ZFTYJS35	
	Correo de Salida	
	josesilva58@writeme.com	
	SHA256	
	468bdf572f6586b2f24783a9b9340bb55836184e09bf8c0cfcceb5687b2b1013 b2e0d0b3fb73a09398df704bb8fc71ad6a437f2803cfc30879346d20b0a05e04 4020c0f5301c573060564e41309bb6a6bc83918c9b6914b5729f5a59d3bbc8d 0815a80fa73286d8c6bf0982471c61833821d9f10a20612deaa134562e7a3cda	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv23-00395-01/	
	https://www.csirt.gob.cl/media/2023/01/2CMV23-00395-01.pdf	

4. Fuerza bruta

CSIRT alerta de ataques de fuerza bruta contra SMTP y comparte IoC	
Alerta de seguridad cibernética	4IIA22-00059-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023
Indicadores de compromiso	
Direcciones IP	
[141.98.11.112] [46.148.40.90] [103.74.103.3] [192.227.217.208] [46.148.40.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iiv23-00059-01/	
https://www.csirt.gob.cl/media/2023/01/4IIV23-00059-01.pdf	

CSIRT alerta de ataques de fuerza bruta contra SMTP y comparte IoC	
Alerta de seguridad cibernética	4IIA22-00060-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023
Indicadores de compromiso	
Direcciones IP	
[46.148.40.90] [141.98.11.112] [80.94.95.206] [45.144.226.76] [36.37.140.118] [192.227.217.208]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iiv23-00059-01/	
https://www.csirt.gob.cl/media/2023/01/4IIV23-00059-01.pdf	

5. Vulnerabilidades

CSIRT comparte vulnerabilidad que afecta a jsonwebtoken	
Alerta de seguridad cibernética	9VSA23-00764-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de enero de 2023
Última revisión	10 de enero de 2023
CVE	
CVE-2022-23529	
Fabricantes	
Jsonwebtoken	
Productos afectados	
JsonWebToken anteriores a la versión 9.0.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00764-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00759-01.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday Enero 2023 de Microsoft		
Alerta de seguridad cibernética	9VSA23-00765-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	10 de enero de 2023	
Última revisión	10 de enero de 2023	
CVE		
CVE-2023-21773	CVE-2023-21741	CVE-2023-21679
CVE-2023-21768	CVE-2023-21755	CVE-2023-21678
CVE-2023-21767	CVE-2023-21780	CVE-2023-21677
CVE-2023-21764	CVE-2023-21779	CVE-2023-21676
CVE-2023-21763	CVE-2023-21745	CVE-2023-21675
CVE-2023-21760	CVE-2023-21762	CVE-2023-21674
CVE-2023-21758	CVE-2023-21761	CVE-2023-21563
CVE-2023-21757	CVE-2023-21752	CVE-2023-21561
CVE-2023-21754	CVE-2023-21527	CVE-2023-21560
CVE-2023-21749	CVE-2023-21743	CVE-2023-21559
CVE-2023-21748	CVE-2023-21524	CVE-2023-21558
CVE-2023-21787	CVE-2023-21759	CVE-2023-21557
CVE-2023-21785	CVE-2023-21753	CVE-2023-21556
CVE-2023-21783	CVE-2023-21746	CVE-2023-21555
CVE-2023-21793	CVE-2023-21739	CVE-2023-21552
CVE-2023-21791	CVE-2023-21733	CVE-2023-21551
CVE-2023-21786	CVE-2023-21744	CVE-2023-21550
CVE-2023-21784	CVE-2023-21742	CVE-2023-21549
CVE-2023-21782	CVE-2023-21738	CVE-2023-21548
CVE-2023-21781	CVE-2023-21737	CVE-2023-21543
CVE-2023-21776	CVE-2023-21736	CVE-2023-21542

	CVE-2023-21774	CVE-2023-21735	CVE-2023-21541
	CVE-2023-21747	CVE-2023-21734	CVE-2023-21540
	CVE-2023-21525	CVE-2023-21732	CVE-2023-21539
	CVE-2023-21792	CVE-2023-21730	CVE-2023-21547
	CVE-2023-21790	CVE-2023-21728	CVE-2023-21546
	CVE-2023-21789	CVE-2023-21726	CVE-2023-21538
	CVE-2023-21788	CVE-2023-21725	CVE-2023-21537
	CVE-2023-21750	CVE-2023-21724	CVE-2023-21536
	CVE-2023-21772	CVE-2023-21683	CVE-2023-21531
	CVE-2023-21766	CVE-2023-21682	CVE-2023-21535
	CVE-2023-21765	CVE-2023-21681	CVE-2023-21532
	CVE-2023-21771	CVE-2023-21680	
	Fabricantes		
	Microsoft		
	Productos afectados		
	Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2012 R2 (Server Core installation) Microsoft Exchange Server 2019 Cumulative Update 12 Microsoft Exchange Server 2019 Cumulative Update 11 Microsoft Exchange Server 2016 Cumulative Update 23 Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 10 Version 20H2 for x64-based Systems 3D Builder		

	Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Microsoft Visio 2016 (32-bit edition) Microsoft Visio 2016 (64-bit edition) Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Visio 2013 Service Pack 1 (32-bit editions) Visual Studio Code Microsoft Exchange Server 2013 Cumulative Update 23 Microsoft Visio 2013 Service Pack 1 (64-bit editions) Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2013 Service Pack 1 Microsoft Office LTSC for Mac 2021 Microsoft Office 2019 for Mac Windows Malicious Software Removal Tool 32-bit Windows Malicious Software Removal Tool 64-bit .NET 6.0 Azure Service Fabric 9.1 Azure Service Fabric 9.0 Azure Service Fabric 8.2
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00765-01/
	https://www.csirt.gob.cl/media/2023/01/9VSA23-00765-01.pdf

CSIRT comparte información de Adobe sobre vulnerabilidades que recibieron actualización de seguridad	
Alerta de seguridad cibernética	9VSA23-00766-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023

CVE

CVE-2023-21579	CVE-2023-21610	CVE-2023-21592
CVE-2023-21581	CVE-2023-21611	CVE-2023-21594
CVE-2023-21585	CVE-2023-21612	CVE-2023-21595
CVE-2023-21586	CVE-2023-21613	CVE-2023-21596
CVE-2023-21604	CVE-2023-21614	CVE-2023-21597
CVE-2023-21605	CVE-2023-21587	CVE-2023-21598
CVE-2023-21606	CVE-2023-21588	CVE-2023-21599
CVE-2023-21607	CVE-2023-21589	CVE-2023-21601
CVE-2023-21608	CVE-2023-21590	CVE-2023-21603
CVE-2023-21609	CVE-2023-21591	

Fabricantes

Adobe

Productos afectados

Acrobat DC 22.003.20282 (Win), 22.003.20281 (Mac) y anteriores.
Acrobat Reader DC 22.003.20282 (Win), 22.003.20281 (Mac) y anteriores.
Acrobat 2020 20.005.30418 y anteriores.
Acrobat Reader 2020 20.005.30418 y anteriores.
Adobe InDesign ID18.0 y anteriores, ID17.4 y anteriores.
Adobe InCopy ID18.0 y anteriores, ID17.4 y anteriores.
Adobe Dimension 3.4.6 y anteriores.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00766-01/
https://www.csirt.gob.cl/media/2023/01/9VSA23-00766-01.pdf

CSIRT comparte información de vulnerabilidades parchadas por Intel para oneAPI Toolkit	
Alerta de seguridad cibernética	9VSA23-00767-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023
CVE	
CVE-2022-40196 CVE-2022-38136 CVE-2022-41342	
Fabricantes	
Intel	
Productos afectados	
Intel oneAPI DPC++/C++ Compiler anterior a 2022.2.1. Intel C++ Compiler Classic anterior a 2021.8.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00767-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00767-01.pdf	

CSIRT comparte información de vulnerabilidades que afectan a productos SAP y que recibieron actualizaciones de seguridad		
Alerta de seguridad cibernética	9VSA23-00768-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	11 de enero de 2023	
Última revisión	11 de enero de 2023	
CVE		
CVE-2022-41203 CVE-2022-41271 CVE-2022-41272 CVE-2023-0014	CVE-2023-0023 CVE-2023-0015 CVE-2023-0022 CVE-2023-0018	CVE-2023-0017 CVE-2023-0016 CVE-2023-0012 CVE-2023-0013
Fabricantes		
SAP		
Productos afectados		
SAP NetWeaver Process Integration (Messaging System) versión 7.50. SAP NetWeaver Process Integration (User Defined Search) versión 7.50. SAP NetWeaver ABAP Server and ABAP Platform SAP BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT. SAP NetWeaver AS for ABAP and ABAP Platform, versiones 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757. SAP NetWeaver AS for Java, versión 7.50. SAP BusinessObjects Business Intelligence Platform (Analysis edition for OLAP) versiones 420, 430. SAP BusinessObjects Business Intelligence Platform (Central management		

	console) versiones 420, 430. SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad) versiones 4.2, 4.3. SAP BusinessObjects Business Intelligence Platform, versión 420. SAP BPC MS 10.0 versiones 800, 810. SAP Host Agent (Windows), Versiones – 7.21, 7.22. SAP Bank Account Management (Manage Banks) versiones 800, 900.
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00768-01/
	https://www.csirt.gob.cl/media/2023/01/9VSA23-00768-01.pdf

CSIRT comparte información de vulnerabilidades parchadas por Cisco para varios de sus productos		
Alerta de seguridad cibernética	9VSA23-00769-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	12 de enero de 2023	
Última revisión	12 de enero de 2023	
CVE		
CVE-2023-20025 CVE-2023-20020 CVE-2023-20026 CVE-2023-20002 CVE-2023-20008 CVE-2023-20045	CVE-2023-20040 CVE-2023-20047 CVE-2023-20043 CVE-2023-20044 CVE-2023-20058	CVE-2023-20019 CVE-2023-20018 CVE-2023-20037 CVE-2023-20038 CVE-2023-20007
Fabricantes		
Cisco		
Productos afectados		
Routers Cisco Small Business RV016, RV042, RV042G, and RV082. Cisco IP Phone 7800 y 8800 series web management interface. Cisco BroadWorks Application Server. Cisco BroadWorks Application Delivery Platform. Cisco BroadWorks Xtended Services Platform. Cisco RV340, RV340W, RV345 y RV345P Dual WAN Gigabit VPN routers. Cisco TelePresence Collaboration Endpoint (CE) Software. Cisco Network Services Orchestrator (NSO) Cisco RoomOS Software. Cisco Webex Room Phone y Cisco Webex Share. Cisco Unified Intelligence Center		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00769-01/		
https://www.csirt.gob.cl/media/2023/01/9VSA23-00769-01.pdf		

CSIRT comparte información de una nueva vulnerabilidad que afecta a Cacti	
Alerta de seguridad cibernética	9VSA23-00770-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023
CVE	
CVE-2022-46169	
Fabricantes	
Cacti	
Productos afectados	
Cacti 1.2.22 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00770-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00770-01.pdf	

CSIRT informa vulnerabilidad parchada en antivirus de Avast, AVG, Avira y Norton	
Alerta de seguridad cibernética	9VSA23-00771-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023
CVE	
CVE-2022-4294	
Fabricantes	
Avast, AVG, Avira y Norton	
Productos afectados	
Norton Antivirus ERASER Engine anteriores a la versión 119.1.5.1, la que soluciona el problema. Avira Security anteriores a la versión 1.1.78, la que soluciona el problema. Avast Antivirus versiones anteriores a la 22.10, la que soluciona el problema. AVG Antivirus versiones anteriores a la 22.10, la que soluciona el problema.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00771-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00771-01.pdf	

6. Concientización

Ciberconsejos para un verano seguro

Durante el verano también debemos preocuparnos por estar ciberseguros, ya sea al navegar por internet como también al usar redes sociales. Diversas son las acciones que puedes tomar para estar seguro en línea y cuidar a además a los más pequeños

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-verano-seguro/

7. 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.

8. 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.

- Romualdo Bizzo
- Manuel Sánchez
- David Zárate
- Francisco Carrasco
- Sebastián Muñoz
- Carlos Brito
- Francisco Flores
- María José Zambrano
- David Torti