CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 197

semana del 7 al 13 de abril de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

**18** IP advertidas en múltiples campañas de phishing y de malware.

## URL ADVERTIDAS

**19** URL asociadas a sitios fraudulentos y campañas de phishing y malware

## PARCHES COMPARTIDOS

**206** Las mitigaciones son útiles en productos de Apple, Google (Android y Chrome), Microsoft, Sophos, Mozilla y SAP.

## HASH REPORTADOS

**9** asociadas a múltiples campañas de phishing con archivos que contienen malware

# CONTENIDO

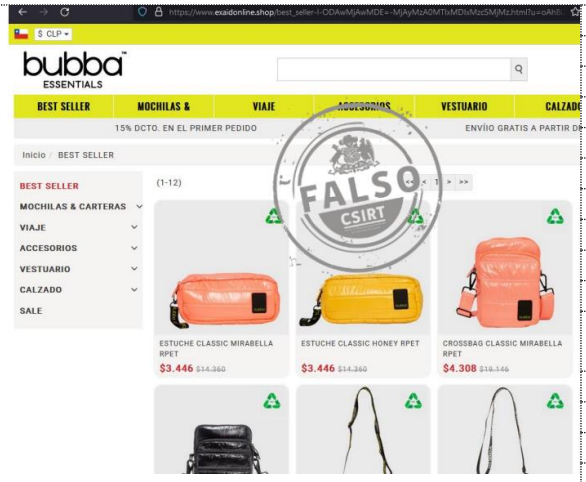




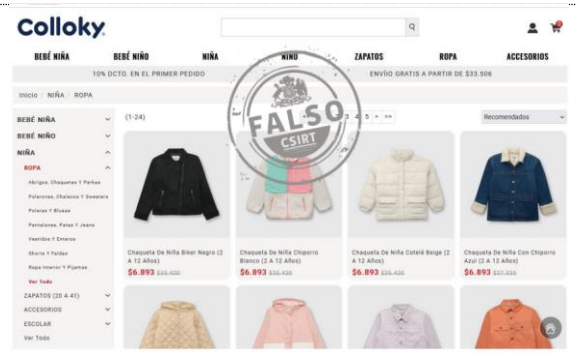
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

## 1. Sitios fraudulentos

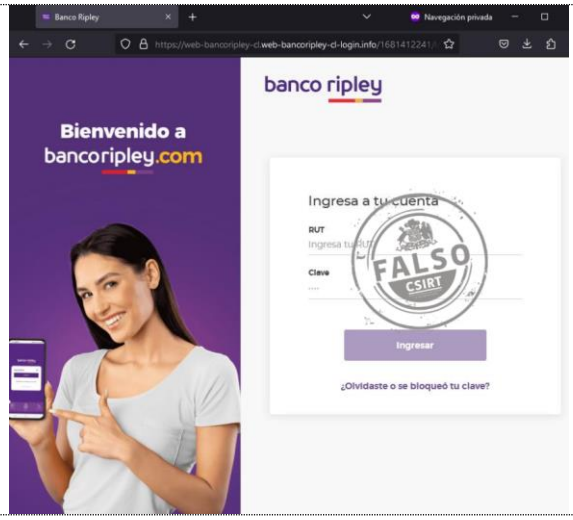

| CSIRT alerta de página fraudulenta que suplanta a Lippi | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01275-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de abril de 2023 |
| Última revisión | 11 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//www.saptofers[.]online/ | |
| **Dirección IP** | |
| [162.222.89.177] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8ffr23-01275-01 | |



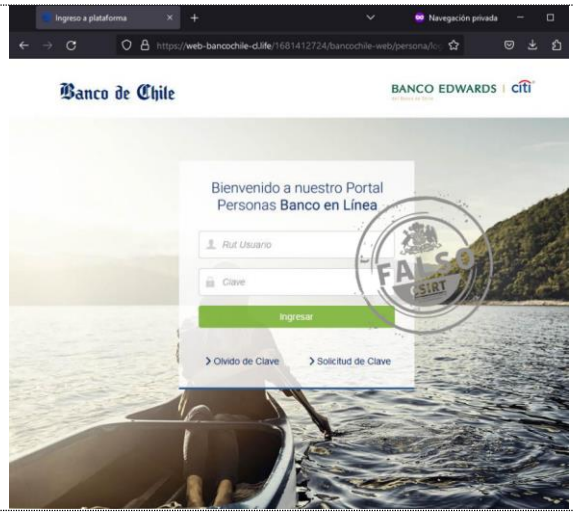

| CSIRT informa de nueva página fraudulenta que suplanta a Bubba Bags | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01276-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de abril de 2023 |
| Última revisión | 12 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https[:]//salebags.mailchimpsites[.]com/?gclid=CjwKCAjwitShBhA6EiwAq3RqAx_kTV3GfAXmW8rs2xeVhBV0keCWnlZIz59-q5Ks_k80k3a6VgtxRRoCNasQAvD_BwE | |
| **URL sitio falso** | |
| https[:]//www.exaidonline[.]shop/?u=oAhBi2q3bYU= | |
| **Dirección IP** | |
| [162.218.176.59] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8ffr23-01276-01 | |




| CSIRT alerta de sitio fraudulento que suplanta a Colloky | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01277-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de abril de 2023 |
| Última revisión | 12 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//www.vetemcam[.]online | |
| **Dirección IP** | |
| [167.160.3.13] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8ffr23-01277-01 | |

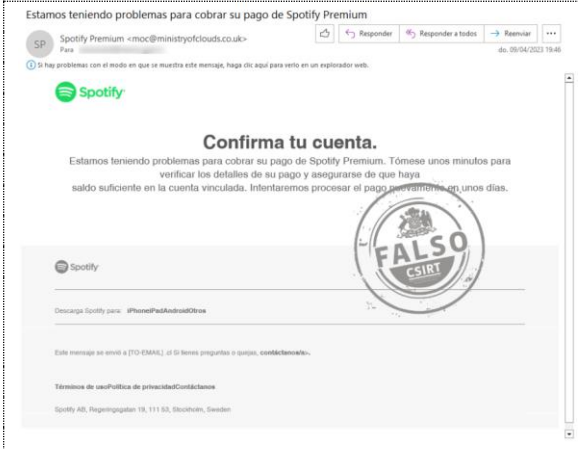



| CSIRT alerta de nueva página fraudulenta que suplanta a Banco Ripley | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01278-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//web-bancoripley-cl.web-bancoripley-cl-login[.]info/1681412241/login/index.html | |
| **Dirección IP** | |
| [172.67.133.184] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8ffr23-01278-01 | |



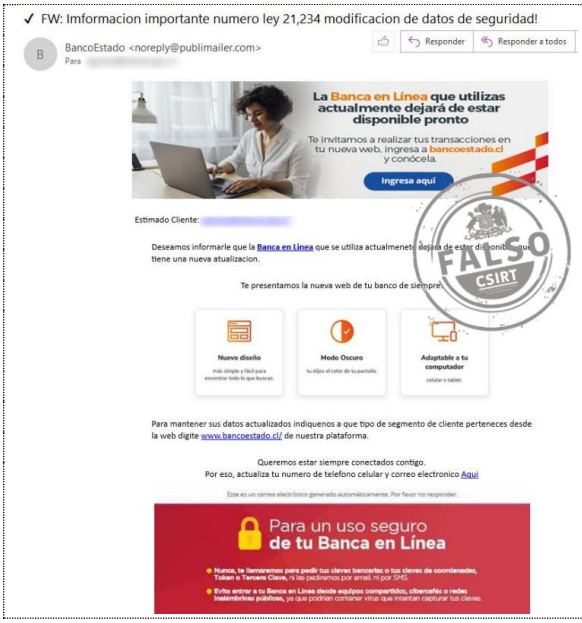

| CSIRT alerta de sitio fraudulento que suplanta al Banco de Chile | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01279-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//web-bancochile-cl[.]life/1681412724/bancochile-web/persona/login/index.html/login | |
| **Dirección IP** | |
| [104.21.46.118] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8ffr23-01279-01 | |

## 2. Phishing



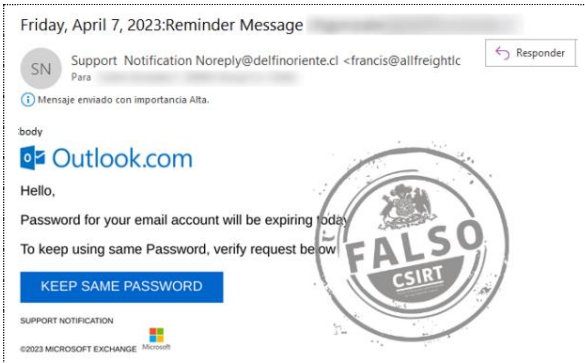

| CSIRT alerta de campaña de phishing que suplanta a Spotify | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00780-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |
| **URL sitio falso** | |
| https[:]//www.carlsencanvas.com/clpremiumes_brand_contextualspotify/cl_premiumfactura1/?view=login&appIdKey=fcd00c0656cc490&country= | |
| **URL redirección** | |
| https[:]//letrazoom.com/yjwcsHR | |
| **Dirección IP** | |
| [13.249.85.88] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00780-01/ | |


| CSIRT alerta de campaña de phishing que suplanta a Zimbra | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00781-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//firebasestorage.googleapis.com/v0/b/oiuuyytrrteertyu.appspot.com/o/index.html?alt=media&token=87c0b2ef-b50a-467b-9bd6-021d581f8a3b | |
| **Dirección IP** | |
| [74.125.132.95] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00781-01/ | |

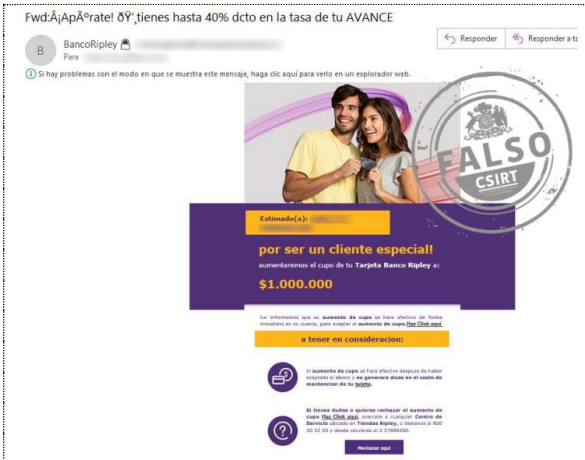



| CSIRT advierte de nueva campaña de phishing que suplanta a BancoEstado | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00782-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https[:]//firebasestorage.googleapis.com/v0/b/oiuuyytrrteertyu.appspot.com/o/index.html?alt=media&token=87c0b2ef-b50a-467b-9bd6-021d581f8a3b | |
| **Dirección IP** | |
| [74.125.132.95] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00782-01/ | |


| CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00783-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https[:]//clubmenthalist[.]com/promocion/cuenta-ooqn/ | |
| **URL sitio falso** | |
| https[:]//nwmmayorsa[.]com/1681160466/imagenes/_personas/home/default.asp | |
| **Dirección IP** | |
| [67.23.242.202] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00783-01/ | |




| CSIRT alerta de campaña de phishing que suplanta a Microsoft Outlook | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00784-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https[:]//m.exactag[.]com/cl.aspx?extProvApi=b2c&extProvID=99&extPu=ew-email&extLi=promo_14-2023_de-DE_sixt&url=https%3A%2F%2Fsimiaestudio.com/%2Fwp-admin%2Fcss%2F/qtcxkc%2F%2F%2F%2FY2hnb256YWxlekBkZWxmaW5vcmllbnRlLmNs<br>https[:]//simiaestudio[.]com//wp-admin/css//qtcxkc////Y2hnb256YWxlekBkZWxmaW5vcmllbnRlLmNs?et_uk=c7849600a47042aab8be962e224c10f3 | |
| **URL sitio falso** | |
| https[:]//xiq5hzxl3l6410c7eae98a6.ainnr.ru/ID-6436bbfce4245 | |
| **Dirección IP** | |
| [172.67.138.107] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00784-01/ | |




| CSIRT alerta de campaña de phishing que suplanta a Banco Ripley | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00785-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https[:]//bit[.]ly/3KWZi4k?l=www.bancoripley.cl | |
| **URL sitio falso** | |
| https[:]//web.bancoripley.cl.berleymate.co[.]nz/1681404303/login | |
| **Dirección IP** | |
| [185.184.154.1] | |
| **Enlace para revisar IoC:** | |
| https://www.csirt.gob.cl/alertas/8fph23-00785-01/ | |

## 3. Ataques de Fuerza Bruta


| CSIRT alerta de ataques de fuerza bruta contra SMTP | |
|---|---|
| Alerta de seguridad cibernética | 4IIA22-00066-01 |
| Clase de alerta | Intentos de Intrusión |
| Tipo de incidente | Intentos de acceso – Fuerza bruta |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **Direcciones IP** | |
| 185.225.73.83<br>141.98.10.60<br>194.87.84.62<br>176.111.173.56<br>193.56.29.192<br>212.87.204.201 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/4iia22-00066-01/ | |

## 4. Vulnerabilidades


| CSIRT comparte información de vulnerabilidades parchadas por Apple en iOS 16.4.1 y en iPadOS 16.4.1 | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00811-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |
| **CVE** | |
| CVE-2023-28206<br>CVE-2023-28205 | |
| **Fabricantes** | |
| Apple | |
| **Productos afectados** | |
| iPhone 8 y posterior, iPad Pro (todos), iPad Air 3ra generación y posteriores, iPad 5ta generación y posteriores, iPad mini 5ta generación y posteriores. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00811-01/ | |


| CSIRT comparte información de vulnerabilidades parchadas en Google Chrome 112 | | |
|---|---|---|
| Alerta de seguridad cibernética | 9VSA23-00812-01 | |
| Clase de alerta | Vulnerabilidad | |
| Tipo de incidente | Sistema y/o Software Abierto | |
| Nivel de riesgo | Alto | |
| TLP | Blanco | |
| Fecha de lanzamiento original | 10 de abril de 2023 | |
| Última revisión | 10 de abril de 2023 | |
| **CVE** | | |
| CVE-2023-1810<br>CVE-2023-1811<br>CVE-2023-1812<br>CVE-2023-1813<br>CVE-2023-1814 | CVE-2023-1815<br>CVE-2023-1816<br>CVE-2023-1817<br>CVE-2023-1818<br>CVE-2023-1819 | CVE-2023-1820<br>CVE-2023-1821<br>CVE-2023-1822<br>CVE-2023-1823 |
| **Fabricantes** | | |
| Google | | |
| **Productos afectados** | | |
| Google Chrome. | | |
| **Enlaces para revisar el informe:** | | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00812-01/ | | |


| CSIRT comparte vulnerabilidades parchadas en la actualización de seguridad de Android de abril 2023 | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00813-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de abril de 2023 |
| Última revisión | 10 de abril de 2023 |

**CVE**

| | | |
|---|---|---|
| CVE-2021-0872 | CVE-2022-33917 | CVE-2023-20967 |
| CVE-2021-0873 | CVE-2022-36449 | CVE-2023-21080 |
| CVE-2021-0874 | CVE-2022-38181 | CVE-2023-21081 |
| CVE-2021-0875 | CVE-2022-40503 | CVE-2023-21082 |
| CVE-2021-0876 | CVE-2022-40532 | CVE-2023-21083 |
| CVE-2021-0878 | CVE-2022-41757 | CVE-2023-21084 |
| CVE-2021-0879 | CVE-2022-42716 | CVE-2023-21085 |
| CVE-2021-0880 | CVE-2022-4696 | CVE-2023-21086 |
| CVE-2021-0881 | CVE-2022-47335 | CVE-2023-21087 |
| CVE-2021-0882 | CVE-2022-47336 | CVE-2023-21088 |
| CVE-2021-0883 | CVE-2022-47337 | CVE-2023-21089 |
| CVE-2021-0884 | CVE-2022-47338 | CVE-2023-21090 |
| CVE-2021-0885 | CVE-2023-20652 | CVE-2023-21091 |
| CVE-2022-20463 | CVE-2023-20653 | CVE-2023-21092 |
| CVE-2022-20471 | CVE-2023-20654 | CVE-2023-21093 |
| CVE-2022-32599 | CVE-2023-20655 | CVE-2023-21094 |
| CVE-2022-33231 | CVE-2023-20656 | CVE-2023-21096 |
| CVE-2022-33269 | CVE-2023-20657 | CVE-2023-21097 |
| CVE-2022-33270 | CVE-2023-20909 | CVE-2023-21098 |
| CVE-2022-33288 | CVE-2023-20935 | CVE-2023-21099 |
| CVE-2022-33289 | CVE-2023-20941 | CVE-2023-21100 |
| CVE-2022-33302 | CVE-2023-20950 | CVE-2023-21630 |

**Fabricantes**

Google

**Productos afectados**

Productos que usan el sistema Operativo Android.

**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00813-01/


| CSIRT comparte las vulnerabilidades parchadas por Microsoft en su Update Tuesday de Abril | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00814-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 11 de abril de 2023 |
| Última revisión | 11 de abril de 2023 |

**CVE**

| | | |
|---|---|---|
| CVE-2023-21729 | CVE-2023-28254 | CVE-2023-28229 |
| CVE-2023-28304 | CVE-2023-28275 | CVE-2023-28227 |
| CVE-2023-23375 | CVE-2023-28276 | CVE-2023-28224 |
| CVE-2023-28300 | CVE-2023-28252 | CVE-2023-28226 |
| CVE-2023-28292 | CVE-2023-28274 | CVE-2023-28225 |
| CVE-2023-28291 | CVE-2023-28277 | CVE-2023-28223 |
| CVE-2023-28313 | CVE-2023-28250 | CVE-2023-28222 |
| CVE-2023-28312 | CVE-2023-28273 | CVE-2023-28221 |
| CVE-2023-28287 | CVE-2023-28249 | CVE-2023-28220 |
| CVE-2023-24893 | CVE-2023-28272 | CVE-2023-28219 |
| CVE-2023-28314 | CVE-2023-28271 | CVE-2023-28218 |
| CVE-2023-28299 | CVE-2023-28247 | CVE-2023-28217 |
| CVE-2023-28296 | CVE-2023-28248 | CVE-2023-28216 |
| CVE-2023-28263 | CVE-2023-28269 | CVE-2023-24931 |
| CVE-2023-28262 | CVE-2023-28270 | CVE-2023-24929 |
| CVE-2023-28260 | CVE-2023-28246 | CVE-2023-24887 |
| CVE-2023-28311 | CVE-2023-28268 | CVE-2023-24928 |
| CVE-2023-28309 | CVE-2023-28244 | CVE-2023-24886 |
| CVE-2023-28308 | CVE-2023-28266 | CVE-2023-24927 |
| CVE-2023-28307 | CVE-2023-28267 | CVE-2023-24885 |
| CVE-2023-28306 | CVE-2023-28243 | CVE-2023-24926 |
| CVE-2023-28305 | CVE-2023-28241 | CVE-2023-24884 |
| CVE-2023-28295 | CVE-2023-28240 | CVE-2023-24925 |
| CVE-2023-28302 | CVE-2023-28236 | CVE-2023-24883 |
| CVE-2023-28298 | CVE-2023-28238 | CVE-2023-24924 |
| CVE-2023-28297 | CVE-2023-28237 | CVE-2023-24914 |
| CVE-2023-28293 | CVE-2023-28232 | CVE-2023-24912 |
| CVE-2023-28288 | CVE-2023-28235 | CVE-2023-24860 |
| CVE-2023-28285 | CVE-2023-28231 | CVE-2023-23384 |
| CVE-2023-28256 | CVE-2023-28234 | CVE-2023-21769 |
| CVE-2023-28278 | CVE-2023-28233 | CVE-2023-21727 |
| CVE-2023-28255 | CVE-2023-28228 | CVE-2023-21554 |
| CVE-2023-28253 | | |

**Fabricante**

Microsoft

**Productos afectados**

.NET 6.0
.NET 7.0
Azure Machine Learning
Azure Service Connector
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Malware Protection Engine

| | |
|---|---|
| | Microsoft ODBC Driver 17 for SQL Server<br>Microsoft ODBC Driver 18 for SQL Server<br>Microsoft Office 2019 for 32-bit editions<br>Microsoft Office 2019 for 64-bit editions<br>Microsoft Office 2019 for Mac<br>Microsoft Office LTSC 2021 for 32-bit editions<br>Microsoft Office LTSC 2021 for 64-bit editions<br>Microsoft Office LTSC for Mac 2021<br>Microsoft OLE DB Driver 18 for SQL Server<br>Microsoft OLE DB Driver 19 for SQL Server<br>Microsoft Publisher 2013 Service Pack 1 (32-bit editions)<br>Microsoft Publisher 2013 Service Pack 1 (64-bit editions)<br>Microsoft Publisher 2013 Service Pack 1 RT<br>Microsoft Publisher 2016 (32-bit edition)<br>Microsoft Publisher 2016 (64-bit edition)<br>Microsoft SharePoint Enterprise Server 2013 Service Pack 1<br>Microsoft SharePoint Enterprise Server 2016<br>Microsoft SharePoint Foundation 2013 Service Pack 1<br>Microsoft SharePoint Server 2019<br>Microsoft SharePoint Server Subscription Edition<br>Microsoft SQL Server 2008 for 32-bit Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2008 for x64-Based Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2008 R2 for 32-Bit Systems Service Pack 3 (QFE)<br>Microsoft SQL Server 2008 R2 for x64-Based Systems Service Pack 3 (QFE)<br>Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)<br>Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)<br>Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)<br>Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)<br>Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)<br>Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)<br>Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connectivity Pack<br>Microsoft SQL Server 2017 for x64-based Systems (CU 31)<br>Microsoft SQL Server 2017 for x64-based Systems (GDR)<br>Microsoft SQL Server 2019 for x64-based Systems (CU 18)<br>Microsoft SQL Server 2019 for x64-based Systems (GDR)<br>Microsoft SQL Server 2022 for x64-based Systems (GDR)<br>Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)<br>Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)<br>Microsoft Visual Studio 2022 version 17.0<br>Microsoft Visual Studio 2022 version 17.2<br>Microsoft Visual Studio 2022 version 17.4<br>Microsoft Visual Studio 2022 version 17.5<br>Raw Image Extension<br>Remote Desktop client for Windows Desktop<br>Send Customer Voice survey from Dynamics 365<br>Visual Studio Code<br>Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems |

| | |
|---|---|
| | Windows 10 Version 20H2 for 32-bit Systems<br>Windows 10 Version 20H2 for ARM64-based Systems<br>Windows 10 Version 20H2 for x64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems<br>Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 version 21H2 for ARM64-based Systems<br>Windows 11 version 21H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2022<br>Windows Server 2022 (Server Core installation) |
| | **Enlaces para revisar el informe:** |
| | https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00814-01/ |


| | |
|---|---|
| **CSIRT comparte vulnerabilidades parchadas en Sophos Web Alliance versión 4.3.10.4** | |
| Alerta de seguridad cibernética | 9VSA23-00815-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de abril de 2023 |
| Última revisión | 12 de abril de 2023 |
| **CVE** | |
| CVE-2023-1671<br>CVE-2022-4934<br>CVE-2020-36692 | |
| **Fabricante** | |
| Sophos | |
| **Productos afectados** | |
| Sophos Web Alliance, versiones anteriores a la 4.3.10.4. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00815-01/ | |


| CSIRT comparte vulnerabilidades parchadas en Mozilla Firefox 112, Firefox ESR 102.10 | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00816-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de abril de 2023 |
| Última revisión | 12 de abril de 2023 |

**CVE**

| | | |
|---|---|---|
| CVE-2023-29531 | CVE-2023-29538 | CVE-2023-29545 |
| CVE-2023-29532 | CVE-2023-29539 | CVE-2023-29546 |
| CVE-2023-29533 | CVE-2023-29540 | CVE-2023-29547 |
| CVE-2023-29534 | CVE-2023-29541 | CVE-2023-29548 |
| CVE-2023-29535 | CVE-2023-29542 | CVE-2023-29549 |
| CVE-2023-29536 | CVE-2023-29543 | CVE-2023-29550 |
| CVE-2023-29537 | CVE-2023-29544 | CVE-2023-29551 |

**Fabricante**

Mozilla

**Productos afectados**

Versiones anteriores a Firefox 112, Firefox for Android 112 y Focus for Android 112, y Firefox ESR anterior a Firefox ESR 102.10.

**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00816-01/


| CSIRT comparte vulnerabilidades parchadas en productos SAP | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00817-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 12 de abril de 2023 |
| Última revisión | 12 de abril de 2023 |

**CVE**

CVE-2023-27267
CVE-2023-28765
CVE-2023-29186

**Fabricante**

SAP

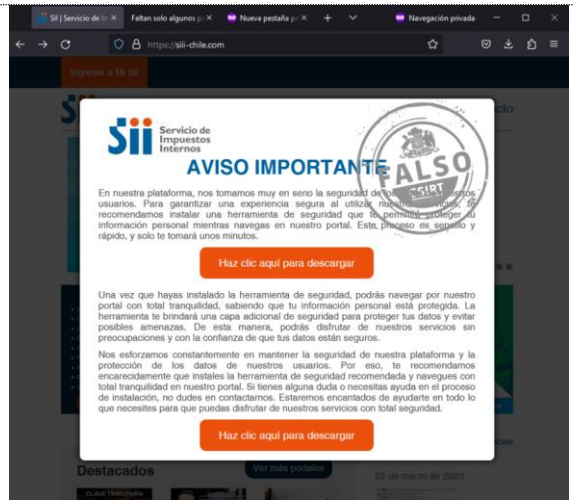
**Productos afectados**

SAP Diagnostics Agent y SAP BusinessObjects Business Intelligence Platform

**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00817-01/

## 5. Malware




| CSIRT alerta de una nueva campaña de phishing con malware, que suplanta al SII | |
|---|---|
| Alerta de seguridad cibernética | 2CMV23-00408-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de abril de 2023 |
| Última revisión | 13 de abril de 2023 |
| **Indicadores de compromiso** | |
| **URL-Dominio** | |
| https://siii-chile.com/<br>https://www.grafoce.com/scripts/index.php?id=2<br>file:\\139.162.73.58@80\YtmpEoBw\Herramienta_de_Seguridad_SII.jse<br>https://www.grafoce.com/wp-contents/execution.php?tag=russian | |
| **SHA256** | |
| e1d2e20285cf909e7075665104948b6ca5c47b356cde4babe06ef91637e743b3<br>209e96742311be142f2ad42f63250aab879a4518978e4d7d74c6859730595ec039<br>5b6bf1b3a8155aaaca12672272c976a29854d12bdeac948e8d6d0059e81cd2 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2cmv23-00408-01/ | |
| https://www.csirt.gob.cl/media/2023/04/2CMV23-00408-01.pdf | |

## 6. Concientización

### Ciberconsejos para no caer en el smishing

Como smishing se conoce a una forma de estafa virtual, que tal como el phishing, busca convencernos de entregar nuestros datos personales o hacer clic en enlaces maliciosos, para descargar programas perjudiciales o permitir a delincuentes tomar control de nuestras cuentas en redes sociales o bancarias. Es importante que estemos al tanto de este tipo de estafa para así evitar caer en ella. Por eso los publicamos esta semana en nuestra web de Recomendaciones: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-no-caer-en-el-smishing/

## Ciberdiccionario Volumen 32

Redes neuronales, minería de datos, tabletop exercise y brecha de datos son los nuevos términos que sumamos a nuestro Ciberdiccionario en su edición 32, disponible también en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-32/.




## 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.

- Rodrigo Alex López Pineda
- César Alberto Camacho Sánchez
- Gabriel Matias Yuseff Campusano
- Christopher Pérez
- Miguel Saldias Cossio
- Patricio Rosas Barriga
- María José Farfán Márquez
- Claudia Fernández Carvajal
- María Gabriela Fernández
- Agustín Covarrubias Izquierdo