



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 237

semana del 12 al 18 de enero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

14

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

93

Las mitigaciones son útiles en productos de QNAP, Adobe, Juniper, Google, Citrix, Atlassian y VMware.



HASH REPORTADOS

12

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



CONTENIDO

1. Malware.....	3
2. Sitios fraudulentos.....	4
3. Phishing	6
4. Vulnerabilidades.....	7
5. Noticias y concientización.....	11
6. Recomendaciones y buenas prácticas	12
7. Muro de la Fama	13

11111<

1. Malware

[SPAM] Citación de justicia para comparecemento ante el tribunal de justicia de Santiago.

Poder Judicial - República de Chile <support@onthebalmedia.es>
 Para <onthebalmedia.es>

Poder Judicial
 Republica del Chile

Estimado Ciudadano

Atencion

Citacion para comparecemento ante el tribunal de justicia de Santiago, en Audiencia publica N2800122023/24 el dia 22/01/2024 Citación **2820124/002**.
 Para mas informacion vea el anexo online en el siguiente archivo abajo.

Información de citación: [CitacionN°2820124/002.zip](#)

El archivo .zip solo estará disponible durante 7 días, si no lo visualiza se entenderá conforme a la acusación.
 La falta de presentación de una defensa resultará en la detención automática.

Todos los derechos reservados, Poder Judicial de Chile



CSIRT alerta de nueva campaña de phishing con malware, que suplanta al Poder Judicial

Alerta de seguridad cibernética	2CMV23-00439-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 enero, 2024
Última revisión	12 enero, 2024

Indicadores de compromiso

URL-Dominio

[https://rao-romania\[.\]com/citacion/republicachilepoderjudicial/?hash={mail}](https://rao-romania[.]com/citacion/republicachilepoderjudicial/?hash={mail})
[https://citrustalent\[.\]com/pk/citacionpoderjudicl.zip?999128620](https://citrustalent[.]com/pk/citacionpoderjudicl.zip?999128620)

SHA256

5a77ae65d77068dee0b029678b84f0234c4788a4de45e8f6f2390b1f09c7cee4a510907486ad34776ddc8c47e08ebd98e985ff9c41b7aede9c8cdd011160a17d36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068e28e34bdaff077669586dcd4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e77e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a192d51cd32647c1e7d5bc57560b4b6938caf5685bafa157edfc960d26a8e172a

Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/2cmv24-00439-01/>

Fw: Informe Facturación Electrónica (Diciembre) - (7452803)

Deppto.Facturacion <Support-SI@mail6322708.cl>
 Para <onthebalmedia.es>

Estimado contribuyente, su Facturación ya está disponible.

La información del impuesto interno está disponible en formato PDF y Excel. Los hemos adjuntado al cuerpo de este correo. También puedes descargarlo haciendo clic en el siguiente botón.

Tienes hasta el 15 de enero de 2024 para modificar tus datos de facturación de boletas de honorarios electrónicos. Después de esta fecha, no podrás hacer ningún clic.

- [Informe detallado-66322708.pdf](#) - Acrobat Reader
- [Informe detallado-66322708.excel](#) - Microsoft Word

Atentamente,

Atención: Para una mejor visualización, abra en un ordenador (ordenador).



CSIRT alerta de nuevo phishing con malware, que suplanta al SII

Alerta de seguridad cibernética	2CMV24-00440-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 enero, 2024
Última revisión	12 enero, 2024

Indicadores de compromiso

URL-Dominio

[https://ccpt.gov\[.\]ng/wps/01923i6C/0D17F5S33/01F3083.php?hash=66322708-ezintloslagos@interior.gov.cl](https://ccpt.gov[.]ng/wps/01923i6C/0D17F5S33/01F3083.php?hash=66322708-ezintloslagos@interior.gov.cl)
[https://jw-ict\[.\]cl/330215B8F11/776T0231CC/02722.php?/mail/0/inbox/id/AQMkADAwATNiZmYAZC1hNDU4LWRkADc2LTAwAi0wMAoARgAAA1kchXVHhZ5CjfaazERwbi8HANHs14LD%2BI9Bt5SmE8UpN2gAAAIBDAAAA](https://jw-ict[.]cl/330215B8F11/776T0231CC/02722.php?/mail/0/inbox/id/AQMkADAwATNiZmYAZC1hNDU4LWRkADc2LTAwAi0wMAoARgAAA1kchXVHhZ5CjfaazERwbi8HANHs14LD%2BI9Bt5SmE8UpN2gAAAIBDAAAA)
[https://silviza\[.\]cl/mail/F981233/UC1023IF8B/home.php?hash=G-O-V](https://silviza[.]cl/mail/F981233/UC1023IF8B/home.php?hash=G-O-V)

SHA256

5a77ae65d77068dee0b029678b84f0234c4788a4de45e8f6f2390b1f09c7cee4a510907486ad34776ddc8c47e08ebd98e985ff9c41b7aede9c8cdd011160a17d36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068e28e34bdaff077669586dcd4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e77e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a98c1f23e6e3176b902dd0446909a5065cbacbd4b3f15ea831d5b7ab01605bea6

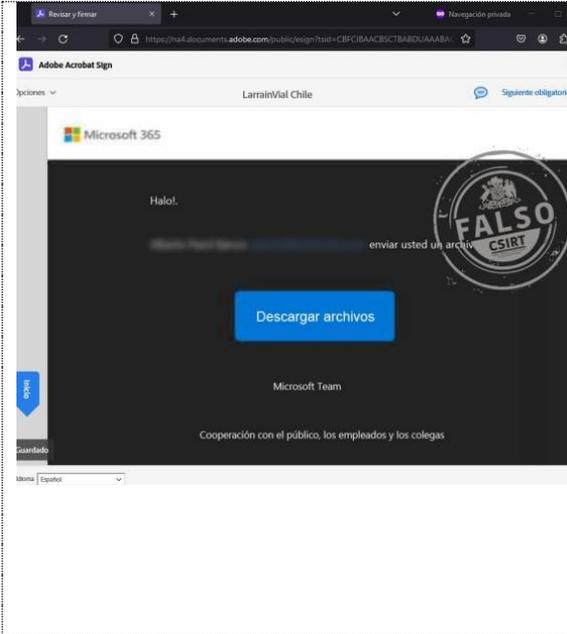
Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/2cmv24-00440-01/>

CONTACTO Y REDES SOCIALES CSIRT

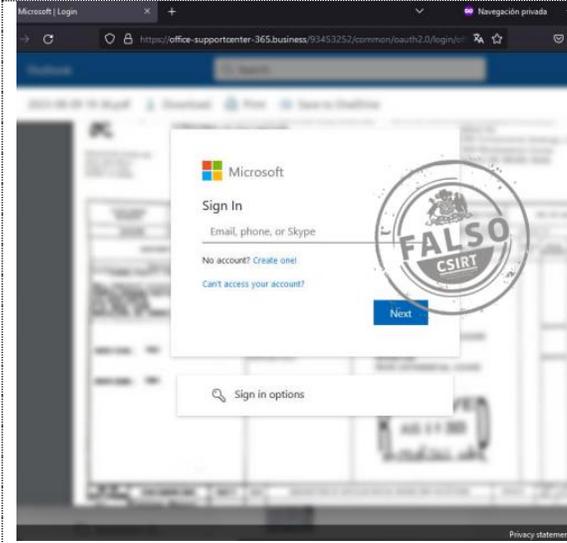
- <https://www.csirt.gob.cl>
- Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
- [@csirtgob](#)
- <https://www.linkedin.com/company/csirt-gob>

2. Sitios fraudulentos



CSIRT alerta de sitio fraudulento que suplanta a Microsoft 365

Alerta de seguridad cibernética	8FFR23-01630-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 enero, 2024
Última revisión	12 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://larrainvial.larrainchile[.]biz/?M7=ap?	
URL de redirección	
https://na4.documents.adobe[.]com/public/esign?tsid=CBFCIBAACBSCTBABDUA AABACAABAARG 75Cg8yAbULiVPEnXjS16jmY-KVpr5PkBOS-JdrEzvVhnfG5CMKy7ZPY9a4_47hpyeLDtVf8JwP2m_5GLzcmPJD8lB54hHHO6T_s35qq_tWOtyA2revbElqCyuVoRZ&	
Dirección IP sitio falso	
[92.205.180.240]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01630-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Microsoft

Alerta de seguridad cibernética	8FFR23-01631-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 enero, 2024
Última revisión	12 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://office-supportcenter-365.business/93453252/common/oauth2.0/login/off/	
URL de redirección	
N/A	
Dirección IP sitio falso	
[104.21.37.254]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01631-01/	

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>



CSIRT alerta de sitio fraudulento que suplanta al Hotel Chalet Suizo, de Vista Hermosa Hoteles

Alerta de seguridad cibernética	8FFR23-01632-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 enero, 2024
Última revisión	12 enero, 2024

Indicadores de compromiso

URL del sitio falso

[https://www.hotelchaletsuizo\[.\]cl/](https://www.hotelchaletsuizo[.]cl/)

URL de redirección

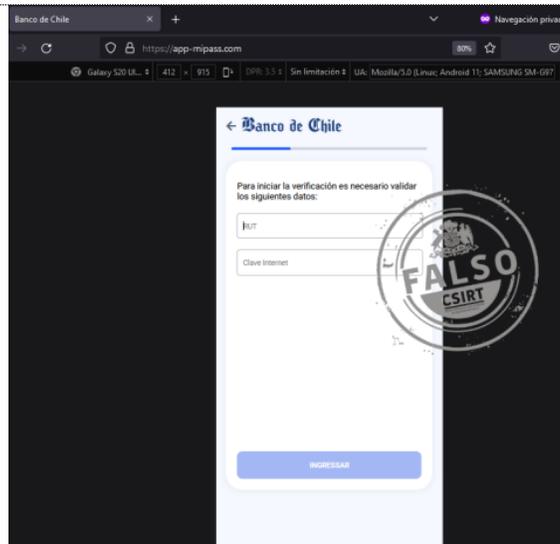
N/A

Dirección IP sitio falso

[162.240.162.0]

Enlace para revisar IoC:

<https://csirt.gob.cl/alertas/8ffr23-01632-01/>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco de Chile

Alerta de seguridad cibernética	8FFR23-01633-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 enero, 2024
Última revisión	17 enero, 2024

Indicadores de compromiso

URL del sitio falso

[https://app-mipass\[.\]com/](https://app-mipass[.]com/)

URL de redirección

N/A

Dirección IP sitio falso

[172.67.159.237]

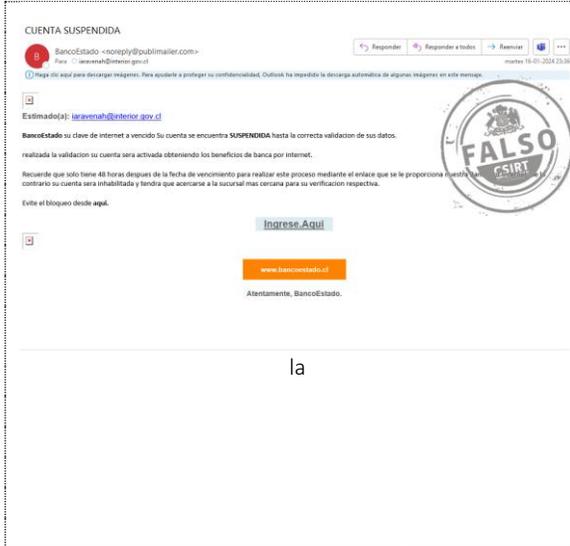
Enlace para revisar IoC:

<https://csirt.gob.cl/alertas/8ffr23-01633-01/>

CONTACTO Y REDES SOCIALES CSIRT

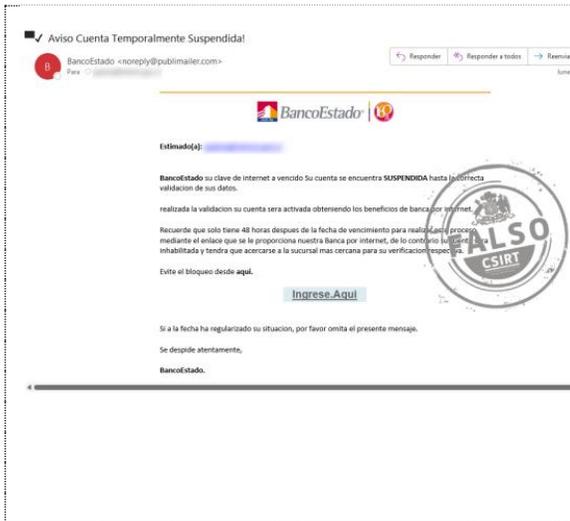
<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>

3. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH24-00922-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 enero, 2024
Última revisión	17 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.sexpressx[.]sa.com/1705494947/imagenes/_personas/home/default.asp	
URL de redirección	
https://procontroltotal[.]com/activacion/cuenta-ajwh/	
Dirección IP sitio falso	
[38.242.247.3]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8fph24-00922-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH24-00923-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 enero, 2024
Última revisión	17 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.theaerie[.]ca/1705514405/imagenes/_personas/home/default.asp	
URL de redirección	
https://procontroltotal[.]com/activacion/cuenta-ajwh/	
Dirección IP sitio falso	
[192.185.138.178]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8fph24-00923-01/	

CONTACTO Y REDES SOCIALES CSIRT

4. Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA24-00953-01
CSIRT comparte información de actualizaciones en productos QNAP

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades en productos de QNAP

Alerta de seguridad cibernética	9VSA24-00953-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 enero, 2024
Última revisión	15 enero, 2024

CVE

CVE-2023-39296	CVE-2023-41287	CVE-2023-47559
CVE-2022-43634	CVE-2023-41288	CVE-2023-47560

Fabricante

QNAP

Productos afectados

QTS versiones 5.1.x y QuTS hero versiones h5.1.x.
 QuMagie 2.2.x

Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00953-01/>



INFORME DE Vulnerabilidad

9VSA24-00954-01
CSIRT informa de actualizaciones en Adobe Substance 3D Stager

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de actualizaciones de seguridad en Adobe Substance 3D Stager

Alerta de seguridad cibernética	9VSA24-00954-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 enero, 2024
Última revisión	16 enero, 2024

CVE

CVE-2024-20710	CVE-2024-20712	CVE-2024-20714
CVE-2024-20711	CVE-2024-20713	CVE-2024-20715

Fabricante

Adobe

Productos afectados

Adobe Substance 3D Stager

Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00954-01/>

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>



CSIRT comparte información de nuevas vulnerabilidades publicadas por Juniper Networks

Alerta de seguridad cibernética	9VSA24-00955-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 enero, 2024
Última revisión	16 enero, 2024

CVE		
CVE-2016-2183	CVE-2024-21595	CVE-2020-0465
CVE-2019-17571	CVE-2024-21597	CVE-2020-0466
CVE-2020-9493	CVE-2024-21599	CVE-2021-0920
CVE-2021-44228	CVE-2024-21600	CVE-2021-26691
CVE-2021-44832	CVE-2024-21601	CVE-2021-34798
CVE-2022-22164	CVE-2024-21602	CVE-2021-3564
CVE-2022-23302	CVE-2024-21603	CVE-2021-3573
CVE-2022-23305	CVE-2024-21604	CVE-2021-3621
CVE-2022-23307	CVE-2024-21606	CVE-2021-3752
CVE-2023-26464	CVE-2024-21607	CVE-2021-39275
CVE-2023-36842	CVE-2024-21611	CVE-2021-4155
CVE-2024-21585	CVE-2024-21612	CVE-2021-44790
CVE-2024-21587	CVE-2024-21613	CVE-2022-0330
CVE-2024-21589	CVE-2024-21614	CVE-2022-22942
CVE-2024-21591	CVE-2022-21699	CVE-2024-21617
CVE-2024-21594		

Fabricante
 Juniper Networks

Productos afectados
 Juniper Networks Junos OS SRX Series y EX Series:
 Junos OS versiones anteriores a la 20.4R3-S9
 Junos OS 21.2 versiones anteriores a la 21.2R3-S7
 Junos OS 21.3 versiones anteriores a la 21.3R3-S5
 Junos OS 21.4 versiones anteriores a la 21.4R3-S5
 Junos OS 22.1 versiones anteriores a la 22.1R3-S4
 Junos OS 22.2 versiones anteriores a la 22.2R3-S3
 Junos OS 22.3 versiones anteriores a la 22.3R3-S2
 Junos OS 22.4 versiones anteriores a la 22.4R2-S2, 22.4R3.
 Juniper Networks Security Director Insights anteriores a la 23.1R1.
 Juniper Networks CTPView, versiones anteriores a la 9.1R5.
 Routers Juniper Networks Session Smart Router anteriores al SSR-6.2.3-r2.

Enlaces para revisar el informe:
<https://csirt.gob.cl/vulnerabilidades/9vsa24-00955-01/>

CONTACTO Y REDES SOCIALES CSIRT

- <https://www.csirt.gob.cl>
- Teléfonos: 1510 | +(562) 24863850 | Correo: incidentes@interior.gob.cl
- @csirtgob
- <https://www.linkedin.com/company/csirt-gob>



INFORME DE Vulnerabilidad

9VSA24-00956-01
CSIRT informa de actualizaciones para vulnerabilidades en Google Chrome

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades parchadas en Google Chrome	
Alerta de seguridad cibernética	9VSA24-00956-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 enero, 2024
Última revisión	18 enero, 2024
CVE	
CVE-2024-0517	
CVE-2024-0518	
CVE-2024-0519	
Fabricante	
Google	
Productos afectados	
Google Chrome, todas las versiones anteriores a 120.0.6099.234 para Mac, 120.0.6099.224 para Linux y 120.0.6099.224/225 para Windows.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00956-01/	



INFORME DE Vulnerabilidad

9VSA24-00957-01
CSIRT informa de actualizaciones para vulnerabilidades en Citrix NetScaler

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades parchadas para Citrix NetScaler	
Alerta de seguridad cibernética	9VSA24-00957-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 enero, 2024
Última revisión	18 enero, 2024
CVE	
CVE-2023-6548	
CVE-2023-6549	
Fabricante	
Citrix	
Productos afectados	
NetScaler ADC and NetScaler Gateway 14.1 anteriores a 14.1-12.35	
NetScaler ADC and NetScaler Gateway 13.1 anteriores a 13.1-51.15	
NetScaler ADC and NetScaler Gateway 13.0 anteriores a 13.0-92.21	
NetScaler ADC and NetScaler Gateway versión 12.1 (end-of-life)	
NetScaler ADC 13.1-FIPS anteriores a 13.1-37.176	
NetScaler ADC 12.1-FIPS anteriores a 12.1-55.302	
NetScaler ADC 12.1-NDcPP anteriores a 12.1-55.302	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00957-01/	

CONTACTO Y REDES SOCIALES CSIRT

-  <https://www.csirt.gob.cl>
-  Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
-  @csirtgob
-  <https://www.linkedin.com/company/csirt-gob>



INFORME DE Vulnerabilidad

9VSA24-00958-01
CSIRT informa de actualizaciones para Atlassian Confluence Data Center

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades en Atlassian Confluence Data Center and Server		
Alerta de seguridad cibernética	9VSA24-00958-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	18 enero, 2024	
Última revisión	18 enero, 2024	
CVE		
CVE-2022-42252	CVE-2024-21674	CVE-2023-36478
CVE-2023-22527	CVE-2023-43642	CVE-2023-39410
CVE-2020-25649	CVE-2023-6481	CVE-2020-26217
CVE-2022-44729	CVE-2023-6378	CVE-2017-7957
CVE-2021-40690	CVE-2023-46589	CVE-2022-4244
CVE-2023-46589	CVE-2023-34455	CVE-2018-10054
CVE-2023-3635	CVE-2023-34454	CVE-2023-5072
CVE-2023-22526	CVE-2023-34453	CVE-2023-46589
CVE-2024-21672	CVE-2023-36478	CVE-2022-40152
CVE-2024-21673	CVE-2023-5072	
Fabricante		
Atlassian		
Productos afectados		
Bitbucket Data Center		
Bitbucket Server		
Bamboo Data Center and Server		
Jira Data Center and Server		
Jira Service Management Data Center and Server		
Crowd Data Center and Server		
Confluence Data Center		
Confluence Server		
Enlaces para revisar el informe:		
https://csirt.gob.cl/vulnerabilidades/9vsa24-00958-01/		



INFORME DE Vulnerabilidad

9VSA24-00959-01
CSIRT informa parche a vulnerabilidad crítica en VMware Aria Automation

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT informa de parche a vulnerabilidad crítica en VMware Aria Automation	
Alerta de seguridad cibernética	9VSA24-00959-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 enero, 2024
Última revisión	18 enero, 2024
CVE	
CVE-2023-34063	
Fabricante	
VMware	
Productos afectados	
VMware Aria Automation (antes vRealize Automation): 8.11.x, 8.12.x, 8.13.x y 8.14.x.	
VMware Cloud Foundation (Aria Automation) 4.x y 5.x.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00959-01/	

CONTACTO Y REDES SOCIALES CSIRT

- <https://www.csirt.gob.cl>
- Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
- [@csirtgob](https://twitter.com/csirtgob)
- <https://www.linkedin.com/company/csirt-gob>

5. Noticias y concientización

Ciberconsejos para mantener nuestros dispositivos más seguros

Para cuidar tu smartphone, tablet o notebook y la información que está en ellos resguardar, te invitamos a seguir estos consejos. También disponibles en PDF. Estos y otros tips se pueden encontrar siempre aquí: <https://csirt.gob.cl/recomendaciones/>. Recuerden que siempre los pueden compartir con sus compañeros y trabajadores.



6 CIBERCONSEJOS PARA DISPOSITIVOS SEGUROS

- 1 Actualiza el sistema operativo y las aplicaciones de tu dispositivo, incluyendo el antivirus.
- 2 Utiliza contraseñas fuertes y cuando la aplicación lo permita, habilita el doble factor de autenticación.
- 3 Realiza una copia de seguridad de manera periódica. Una buena idea es hacerlo antes de salir de vacaciones.
- 4 Evita usar redes wifi públicas y, en caso de conectarte, nunca realices alguna transacción financiera o comercial.
- 5 Si pierdes tu dispositivo móvil, activa la funcionalidad de búsqueda de dispositivos, como "Find My iPhone" para Apple o "Find My Device" para Android.
- 6 Activa el bloqueo de pantalla en cualquiera de tus dispositivos. Es la puerta de entrada para acceder a tu información.

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

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.

CONTACTO Y REDES SOCIALES CSIRT

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.

- David Soto
- Kevin Isaac Acevedo Vidal
- Pablo Pizarro
- Felipe Cortés
- Pablo Fabres
- Pablo Ignacio Pizarro Cortínez
- Carlos Francisco Tirado Elgueta
- Marcelo Araneda

CONTACTO Y REDES SOCIALES CSIRT