CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 219

semana del 8 al 14 de septiembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

9

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

12

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

87

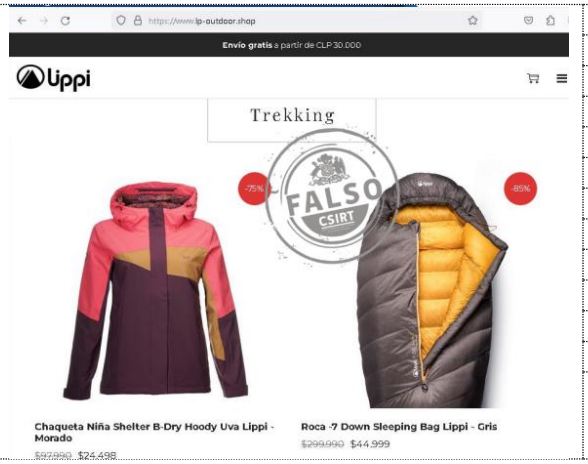
Las mitigaciones son útiles en productos de Microsoft, SAP, Cisco, Google y Mozilla.

CONTENIDO

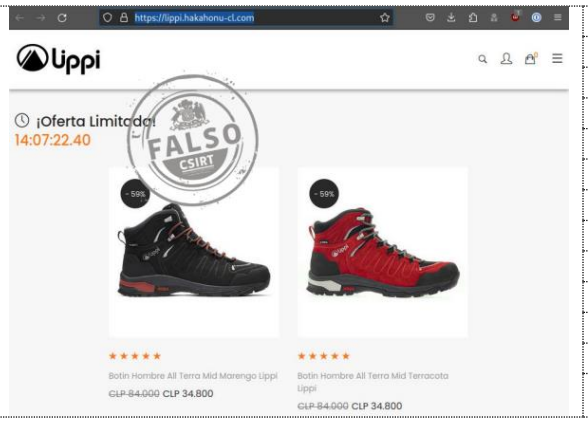
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

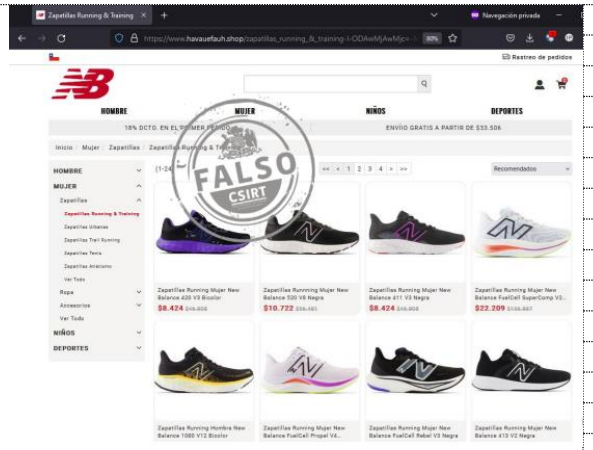
CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01521-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 septiembre, 2023
Última revisión	11 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://personaestado.top/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01521-01/	



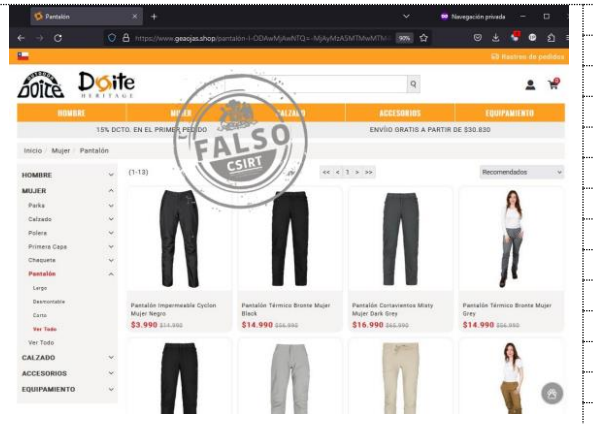
CSIRT alerta ante nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01522-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 septiembre, 2023
Última revisión	11 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lp-outdoor.shop/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01522-01/	



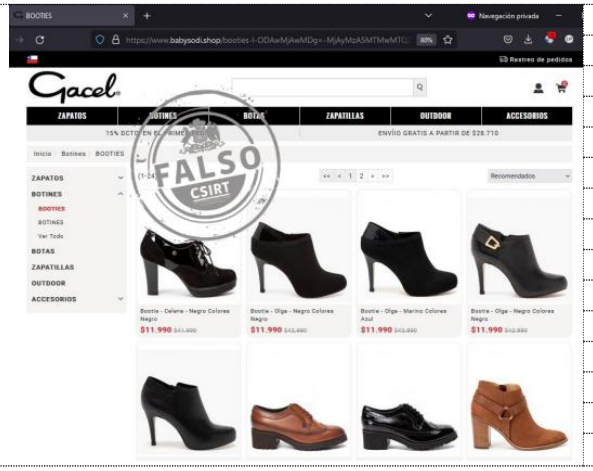
CSIRT alerta de nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01523-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://lippi.hakahonu-cl.com/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01523-01/	



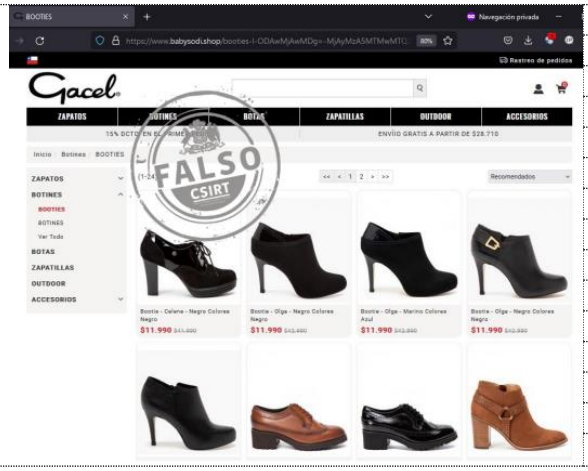
CSIRT alerta de un nuevo sitio fraudulento que suplanta a New Balance	
Alerta de seguridad cibernética	8FFR23-01524-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.havauefauh[.]shop	
Dirección IP	
[195.128.249.9]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01524-01/	



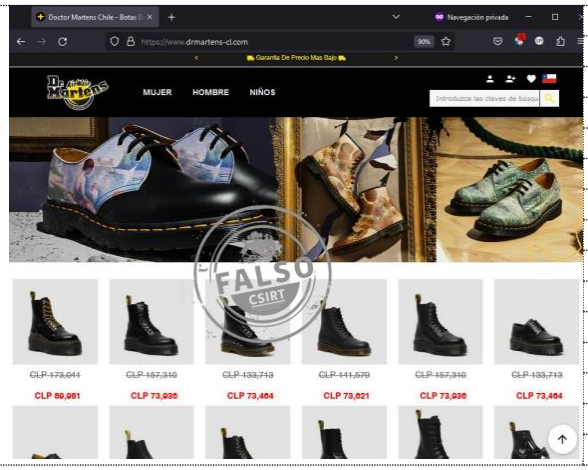
CSIRT alerta de nuevo sitio fraudulento que suplanta a Doite	
Alerta de seguridad cibernética	8FFR23-01525-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
www.geaojas[.]shop/	
Dirección IP	
[23.252.71.103]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01525-01/	



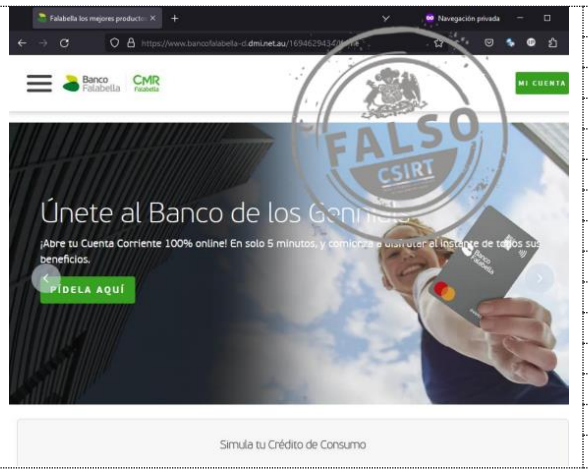
CSIRT alerta de nueva página fraudulenta que suplanta a Gacel	
Alerta de seguridad cibernética	8FFR23-01526-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.babysodi[.]shop	
Dirección IP	
[195.128.249.9]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01526-01/	



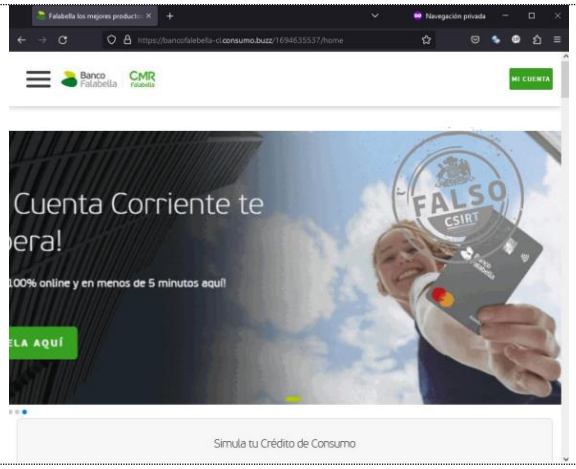
CSIRT alerta de nuevo sitio fraudulento que suplanta a Dr. Martens	
Alerta de seguridad cibernética	8FFR23-01527-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.doctormartenschliecl[.]com/	
Dirección IP	
[165.231.152.143]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01527-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Dr. Martens	
Alerta de seguridad cibernética	8FFR23-01528-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.drmartens-cl[.]com/	
Dirección IP	
[196.196.13.212]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01528-01/	

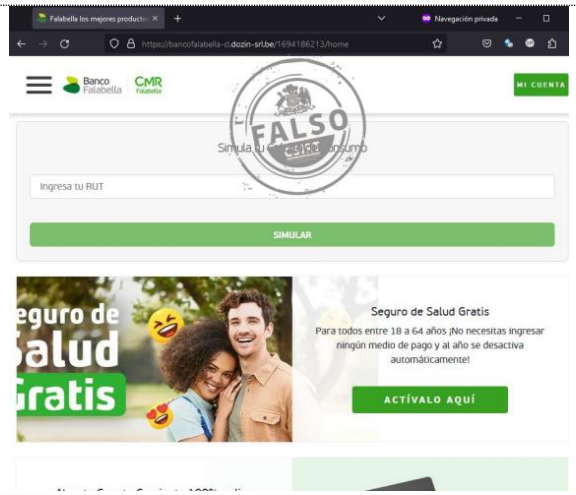


CSIRT alerta de nueva página fraudulenta que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01529-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.bancofalabella-cl.dmi[.]net.au/1694629434/home	
Dirección IP	
[103.20.202.177]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01529-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01530-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 septiembre, 2023
Última revisión	14 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://bancofalebella-cl.consumo[.]buzz/1694635537/home	
Dirección IP	
[104.21.80.6]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01530-01/	

2. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FPH23-00888-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 septiembre, 2023
Última revisión	11 septiembre, 2023
URL redirección	
https://dumepadel[.]pt/bancofalabella/cuenta-slcb/	
URL sitio falso	
https://bancofalabella-cl.dozin-srl[.]be/1694186213/home	
Dirección IP	
[5.189.162.77]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00888-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FPH23-00889-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 septiembre, 2023
Última revisión	11 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://sempel[.]com.br/bancofalabella/cuenta-ceto/	
URL sitio falso	
https://bancofalabella-cl.fandgplasteringinc[.]com/1694441282/home	
Dirección IP sitio falso	
[192.232.216.135]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00889-01/	

3. Vulnerabilidades

CSIRT comparte información de nuevas vulnerabilidades parchadas por Cisco para algunos de sus productos	
Alerta de seguridad cibernética	9VSA23-00895-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 septiembre, 2023
Última revisión	8 septiembre, 2023
CVE	
CVE-2023-20238 CVE-2023-20193 CVE-2023-20194 CVE-2023-20243 CVE-2023-20250 CVE-2023-20263 CVE-2023-20269	
Fabricante	
Cisco	
Productos afectados	
Cisco BroadWorks Application Delivery Platform Cisco BroadWorks Xtended Services Platform Cisco Identity Services Engine (ISE) Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Cisco HyperFlex HX Data Platform Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00895-01/	

CSIRT comparte información de nueva vulnerabilidad crítica que afecta a Google Chrome	
Alerta de seguridad cibernética	9VSA23-00896-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 septiembre, 2023
Última revisión	12 septiembre, 2023
CVE	
CVE-2023-4863	
Fabricante	
Google	
Productos afectados	
Google Chrome 116	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00896-01/	

CSIRT comparte información de vulnerabilidades parchadas en Update Tuesday de Microsoft para septiembre 2023	
Alerta de seguridad cibernética	9VSA23-00897-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 septiembre, 2023
Última revisión	12 septiembre, 2023

CVE

CVE-2023-4863	CVE-2023-38144	CVE-2023-36793	CVE-2023-36759
CVE-2023-41764	CVE-2023-38143	CVE-2023-36792	CVE-2023-36758
CVE-2023-39956	CVE-2023-38142	CVE-2023-36788	CVE-2023-36757
CVE-2023-38164	CVE-2023-38141	CVE-2023-36777	CVE-2023-36756
CVE-2023-38163	CVE-2023-38140	CVE-2023-36773	CVE-2023-36745
CVE-2023-38162	CVE-2023-38139	CVE-2023-36772	CVE-2023-36744
CVE-2023-38161	CVE-2023-36886	CVE-2023-36771	CVE-2023-36742
CVE-2023-38160	CVE-2023-36805	CVE-2023-36770	CVE-2023-36740
CVE-2023-38156	CVE-2023-36804	CVE-2023-36767	CVE-2023-36739
CVE-2023-38155	CVE-2023-36803	CVE-2023-36766	CVE-2023-36736
CVE-2023-38152	CVE-2023-36802	CVE-2023-36765	CVE-2023-35355
CVE-2023-38150	CVE-2023-36801	CVE-2023-36764	CVE-2023-33136
CVE-2023-38149	CVE-2023-36800	CVE-2023-36763	CVE-2023-32051
CVE-2023-38148	CVE-2023-36799	CVE-2023-36762	CVE-2023-29332
CVE-2023-38147	CVE-2023-36796	CVE-2023-36761	CVE-2023-24936
CVE-2023-38146	CVE-2023-36794	CVE-2023-36760	CVE-2022-41303

Fabricante

Microsoft

Productos afectados

.NET and Visual Studio
.NET Core & Visual Studio
.NET Framework
3D Builder
3D Viewer
Azure DevOps
Azure HDInsights
Microsoft Azure Kubernetes Service
Microsoft Dynamics
Microsoft Dynamics Finance & Operations
Microsoft Edge (Chromium-based)
Microsoft Exchange Server
Microsoft Identity Linux Broker
Microsoft Office
Microsoft Office Excel
Microsoft Office Outlook
Microsoft Office SharePoint
Microsoft Office Word
Microsoft Streaming Service
Microsoft Windows Codecs Library
Servicing Stack Updates
Visual Studio
Visual Studio Code
Windows Cloud Files Mini Filter Driver
Windows Common Log File System Driver
Windows Defender

	Windows DHCP Server Windows GDI Windows Internet Connection Sharing (ICS) Windows Kernel Windows Scripting Windows TCP/IP Windows Themes
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00897-01/

CSIRT comparte información de nueva vulnerabilidad crítica en Mozilla Firefox y Thunderbird	
Alerta de seguridad cibernética	9VSA23-00898-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 septiembre, 2023
Última revisión	13 septiembre, 2023
CVE	
CVE-2023-4863	
Fabricante	
Mozilla	
Productos afectados	
Firefox, Firefox ESR, Thunderbird	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00898-01/	

CSIRT comparte información de vulnerabilidades en actualización mensual de seguridad de Adobe			
Alerta de seguridad cibernética	9VSA23-00899-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	14 septiembre, 2023		
Última revisión	14 septiembre, 2023		
CVE			
CVE-2023-29305 CVE-2023-29306	CVE-2023-26369	CVE-2023-38214	CVE-2023-38215
Fabricante			
Adobe			
Productos afectados			
Adobe Connect 12.3 y anteriores. Adobe Acrobat DC 23.003.20284 y anteriores. Adobe Acrobat Reader DC 23.003.20284 y anteriores. Adobe Acrobat 2020 20.005.30516 (Mac) y 20.005.30514 (Win) y anteriores. Adobe Acrobat Reader 2020 20.005.30516 (Mac) y 20.005.30514 (Win) y anteriores.			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00899-01/			

CSIRT comparte información de vulnerabilidades de actualización mensual de SAP para septiembre 2023			
Alerta de seguridad cibernética		9VSA23-00900-01	
Clase de alerta		Vulnerabilidad	
Tipo de incidente		Sistema y/o Software Abierto	
Nivel de riesgo		Alto	
TLP		Blanco	
Fecha de lanzamiento original		14 septiembre, 2023	
Última revisión		14 septiembre, 2023	
CVE			
CVE-2023-40622	CVE-2023-40308	CVE-2021-41183	CVE-2023-37489
CVE-2022-41272	CVE-2023-40621	CVE-2021-41182	CVE-2023-41369
CVE-2023-25616	CVE-2023-40623	CVE-2023-24998	CVE-2023-41368
CVE-2023-40309	CVE-2023-40306	CVE-2023-40624	CVE-2023-41367
CVE-2023-42472	CVE-2021-41184	CVE-2023-40625	
Fabricante			
SAP			
Productos afectados			
SAP Business Client, Versiones -6.5, 7.0, 7.70 SAP BusinessObjects Business Intelligence Platform (Promotion Management), versiones 420,430 SAP NetWeaver Process Integration, Versión –7.50 SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430 SAP CommonCryptoLib, Versiones–8 SAP NetWeaver AS ABAP SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise. SAP Web Dispatcher, Versiones -7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 SAP Content Server, Versiones -6.50, 7.53, 7.54 SAP HANA Database, Versiones –2.0 SAP Host Agent, Versiones –722 SAP Extended Application Services and Runtime (XSA) SAPSSOEXT, Versiones –17 SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface),Versión 420 SAP CommonCryptoLib, Versiones–8 SAP NetWeaver AS ABAP SAP NetWeaver AS Java and ABAP Platform of S/4HANA on-premise. SAP Web Dispatcher, Versiones -7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 SAPContent Server, Versiones -6.50, 7.53, 7.54 SAPHANA Database, Versiones –2.0 SAPHost Agent, Versiones –722 SAPExtended Application Services and Runtime (XSA), versiones SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 SAPSSOEXT, Versiónes –17 SAP PowerDesignerClient, Versión –16.7 SAP BusinessObjects Suite (Installer), Versión –420, 430 SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), versiones S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106 SAPUI5, Versiones –SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200 SAP Quotation Management Insurance (FS-QUO), versiones 400, 510, 700, 800 SAP NetWeaver AS ABAP (applications based on Unified Rendering), versiones SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702, SAP_BASIS 731			

	S4CORE (Manage Purchase Contracts App), Versiones–102, 103, 104, 105, 106, 107 SAP BusinessObjects Business Intelligence Platform (Versión Management System), versiones 430 SAP NetWeaver (Guided Procedures), Versión –7.50 SAP S/4HANA (Create Single Payment application), versiones 100, 101, 102, 103, 104, 105, 106, 107, 108 S4 HANA ABAP (Manage checkbook apps), versiones 102, 103, 104, 105, 106, 107
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00900-01/

4. Noticias y concientización

Alerta de Seguridad de la Información | Ransomware en máquinas virtuales de IFX

Esta semana, el Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior (CSIRT) tomó conocimiento de un comunicado dado a conocer por IFX Networks (propietaria en Chile de la firma Netglobalis), informando que parte de su infraestructura de Colombia sufre actualmente un evento de ransomware, el que ha redundado en la indisponibilidad de servicios también en Chile.

A causa de esta situación, aún en desarrollo, desde el CSIRT hemos compartido recomendaciones en dos alertas de seguridad de la información, que pueden ser revisadas aquí:
10CND23-00108-01: https://www.csirt.gob.cl/noticias/10cnd23-00108-01/.
10CND23-00108-02: https://www.csirt.gob.cl/noticias/10cnd23-00108-02/.

Llamamos a las empresas e instituciones a mantenerse al tanto de la evolución de este problema a través de nuestro sitio web y cuentas en Twitter y LinkedIn.

Llamado a inscripciones para la clasificatoria al OEA Cyber Challenge 2023

Este 2 de octubre se realizará el ejercicio virtual de clasificación para elegir a quienes participarán representando a Chile en el OEA Cyber Challenge, un emocionante ejercicio de ciberseguridad que entrega a quienes participan una oportunidad para demostrar sus habilidades, trabajar en equipo y disputar la corona en nombre de su país.

Para ser parte de esta eliminatoria, solo es necesario ser estudiante, tener entre 18 y 30 años, vivir en Chile y poseer conocimientos básicos de ciberseguridad, redes, programación y sistemas operativos. El período de inscripción termina el 28 de septiembre.

Quienes clasifiquen a la final del OEA Cyber Challenge se enfrentarán a contrincantes de toda América, este 25 y 26 de octubre de manera presencial en la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile.

Inscripciones, aquí: https://oea-cyberchallenge-chile.hackrocks.com/.

Alerta de Seguridad de la Información | Vulnerabilidad crítica en servidores que usan JBoss 4.3.2

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior (CSIRT) informó de su detección de una vulnerabilidad crítica, identificada como Insecure Configuration, en sistemas desarrollados por terceros utilizando el servicio JBoss 4.3.2.

Debido al problema de configuración mencionado, es posible ejecutar código arbitrario en servidores que poseen instalada la aplicación JBoss sin necesidad de autentificación, debido a la exposición pública del controlador de Java Management Extensions (JMX) JMXInvokerServlet.

La información completa está disponible aquí: https://www.csirt.gob.cl/noticias/10cnd23-00107-01/.

5. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

6. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Alexi Contreras Vera
- Pablo Ignacio Pizarro Cortínez
- Fernando Podesta Barrientos
- Julio López Saa
- Alan Lagos Kaune
- Christopher Pérez
- Luis Castillo
- Gerardo Carrizo Tordecilla
- Alonso Ignacio Villalobos González
- Enrique Moraga
- Miguel Morales Saravia
- Bastián Cristóbal Ascencio Caro

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.15 17:08:38 -03'00'