CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 223

semana del 6 al 12 de octubre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

5

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

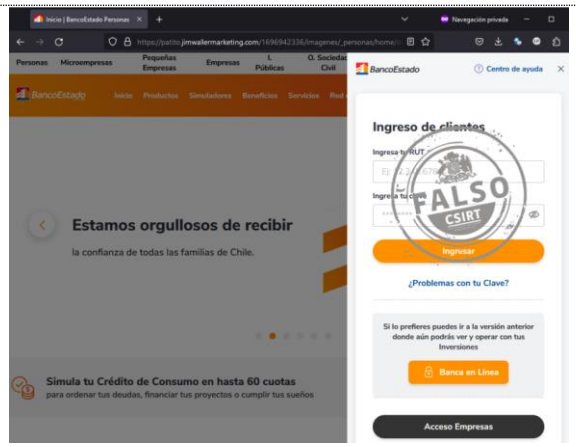
121

Las mitigaciones son útiles en productos de Microsoft, Google, Citrix y varios otros proveedores.

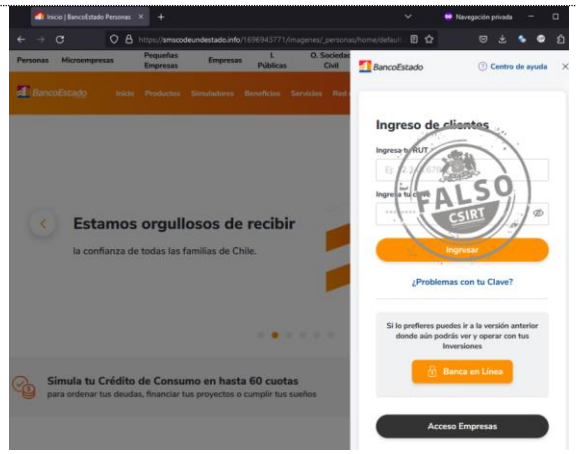
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

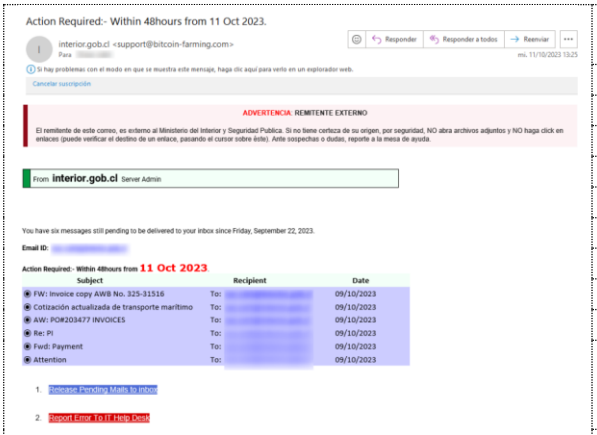
1. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00897-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 octubre, 2023
Última revisión	10 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.jimwallermarketing[.]com/1696942336/imagenes/_personas/home/default.asp	
URL de redirección	
https://promezclas[.]com/activacion/cuenta-wckh/	
Dirección IP sitio falso	
[65.181.111.11]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00897-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00898-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 octubre, 2023
Última revisión	10 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://smscodeundestado[.]info/1696943771/imagenes/_personas/home/default.asp	
URL de redirección	
https://codeundestado[.]com/activacion/cuenta-knnt/	
Dirección IP sitio falso	
[198.27.78.113]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00898-01/	



CSIRT alerta de nueva campaña de phishing con falso aviso de emails pendientes de entrega	
Alerta de seguridad cibernética	8FPH23-00899-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 octubre, 2023
Última revisión	12 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/QmdFYTYL7nVVhP2wHjZdaDsW6BykiLwS6vLA8WHPXh7ueg?filename=sat-desktop.html#csirt@interior.gob.cl	
Dirección IP sitio falso	
[103.54.59.165]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00899-01/	

2. Vulnerabilidades

CSIRT comparte información del Update Tuesday de Microsoft para octubre 2023	
Alerta de seguridad cibernética	9VSA23-00914-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 octubre, 2023
Última revisión	10 octubre, 2023

CVE

CVE-2023-36602	CVE-2023-36568	CVE-2023-36435	CVE-2023-36596
CVE-2023-36720	CVE-2023-36721	CVE-2023-36902	CVE-2023-36603
CVE-2023-36724	CVE-2023-36417	CVE-2023-35349	CVE-2023-36605
CVE-2023-36725	CVE-2023-38171	CVE-2023-36785	CVE-2023-36606
CVE-2023-36431	CVE-2023-36418	CVE-2023-36564	CVE-2023-36697
CVE-2023-36434	CVE-2023-36419	CVE-2023-36565	CVE-2023-36698
CVE-2023-36433	CVE-2023-36730	CVE-2023-36567	CVE-2023-36701
CVE-2023-36557	CVE-2023-36429	CVE-2023-36571	CVE-2023-36702
CVE-2023-36778	CVE-2023-36717	CVE-2023-36572	CVE-2023-36703
CVE-2023-36436	CVE-2023-36718	CVE-2023-36573	CVE-2023-36704
CVE-2023-36576	CVE-2023-36726	CVE-2023-36574	CVE-2023-36706
CVE-2023-36598	CVE-2023-36737	CVE-2023-36575	CVE-2023-36707
CVE-2023-36438	CVE-2023-36415	CVE-2023-36577	CVE-2023-36709
CVE-2023-36563	CVE-2023-36416	CVE-2023-36578	CVE-2023-36710
CVE-2023-36722	CVE-2023-36723	CVE-2023-36579	CVE-2023-36711
CVE-2023-36569	CVE-2023-36728	CVE-2023-36581	CVE-2023-36712
CVE-2023-36570	CVE-2023-41773	CVE-2023-36582	CVE-2023-36713
CVE-2023-36731	CVE-2023-41772	CVE-2023-36583	CVE-2023-36729
CVE-2023-36732	CVE-2023-41771	CVE-2023-36584	CVE-2023-41774
CVE-2023-36566	CVE-2023-41770	CVE-2023-36585	CVE-2023-41769
CVE-2023-41763	CVE-2023-41768	CVE-2023-36589	CVE-2023-41766
CVE-2023-36414	CVE-2023-41767	CVE-2023-36590	CVE-2023-41765
CVE-2023-36561	CVE-2023-36743	CVE-2023-36591	CVE-2023-36789
CVE-2023-44487	CVE-2023-36776	CVE-2023-36592	CVE-2023-36786
CVE-2023-36780	CVE-2023-36790	CVE-2023-36593	CVE-2023-38159
CVE-2023-36420	CVE-2023-38166	CVE-2023-36594	CVE-2023-29348

Fabricante

Microsoft

Productos afectados

.NET 6.0
.NET 7.0
ASP.NET Core 6.0
ASP.NET Core 7.0
Azure DevOps Server 2020.0.2
Azure DevOps Server 2020.1.2
Azure DevOps Server 2022.0.1
Azure HDInsight
Azure Identity SDK for .NET
Azure Identity SDK for Java
Azure Identity SDK for JavaScript
Azure Identity SDK for Python
Azure Network Watcher VM Extension
Azure RTOS GUIX Studio

	Azure RTOS GUIX Studio Installer Application Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Common Data Model SDK for C# Microsoft Common Data Model SDK for Java Microsoft Common Data Model SDK for Python Microsoft Common Data Model SDK for TypeScript Microsoft Dynamics 365 (on-premises) version 9.0 Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 12 Microsoft Exchange Server 2019 Cumulative Update 13 Microsoft ODBC Driver 17 for SQL Server on Linux Microsoft ODBC Driver 17 for SQL Server on MacOS Microsoft ODBC Driver 17 for SQL Server on Windows Microsoft ODBC Driver 18 for SQL Server on Linux Microsoft ODBC Driver 18 for SQL Server on MacOS Microsoft ODBC Driver 18 for SQL Server on Windows Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for Mac Microsoft Office for Android Microsoft Office for Universal Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft OLE DB Driver 18 for SQL Server Microsoft OLE DB Driver 19 for SQL Server Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4) Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR) Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4) Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2017 for x64-based Systems (CU 31) Microsoft SQL Server 2017 for x64-based Systems (GDR) Microsoft SQL Server 2019 for x64-based Systems (CU 22) Microsoft SQL Server 2019 for x64-based Systems (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 8) Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft Visual Studio 2022 version 17.2 Microsoft Visual Studio 2022 version 17.4 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2022 version 17.7 Skype for Business Server 2015 CU13 Skype for Business Server 2019 CU7 Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems

	Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation)Skype for Desktop Webp Image Extensions (Released on Windows and updates Microsoft Store)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00914-01/

CSIRT informa de vulnerabilidades críticas en Citrix NetScaler ADC y NetScaler Gateway	
Alerta de seguridad cibernética	9VSA23-00915-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 octubre, 2023
Última revisión	10 octubre, 2023
CVE	
CVE-2023-4966 CVE-2023-4967	
Fabricante	
Citrix	
Productos afectados	
NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50 NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.15 NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.19 NetScaler ADC 13.1-FIPS before 13.1-37.164 NetScaler ADC 12.1-FIPS before 12.1-55.300 NetScaler ADC 12.1-NDcPP before 12.1-55.300	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00915-01/	

CSIRT comparte información de vulnerabilidades parchadas en Google Chrome 118			
Alerta de seguridad cibernética	9VSA23-00916-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	12 octubre, 2023		
Última revisión	12 octubre, 2023		
CVE			
CVE-2023-5218	CVE-2023-5483	CVE-2023-5479	CVE-2023-5477
CVE-2023-5487	CVE-2023-5481	CVE-2023-5485	CVE-2023-5486
CVE-2023-5484	CVE-2023-5476	CVE-2023-5478	CVE-2023-5473
CVE-2023-5475	CVE-2023-5474		
Fabricante			
Google			
Productos afectados			
Google Chrome			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00916-01/			

CSIRT comparte información de vulnerabilidad HTTP/2 Rapid Reset Attack	
Alerta de seguridad cibernética	9VSA23-00917-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 octubre, 2023
Última revisión	12 octubre, 2023
CVE	
CVE-2023-44487	
Fabricante	
Varios	
Productos afectados	
Software de: Cloudfare Amazon Web Services Google Cloud F5 (NGINX Open Source, NGINX Plus y relacionados). Alibaba Tengine Apache Tomcat 10.x Swift NIO Jetty Debian Red Hat Ubuntu Microsoft Netty Entre otros.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00917-01/	

3. Noticias y concientización

Alrededor de 500 espectadores en vivo tuvo nuestra primera charla de ciclo por el Mes de la Ciberseguridad

Este octubre comenzamos un ciclo de charlas transmitidas en vivo cada viernes a las 10 de la mañana, con conceptos básicos de seguridad de la información, enmarcadas en el Mes de la Ciberseguridad y aptas para todo tipo de público, sin necesitar de contar con conocimientos de tecnología o ciberseguridad.

La primera estuvo a cargo de Hernán Espinoza, auditor del CSIRT, y fue vista por casi 500 personas en vivo, sumando cientos de vistas más en YouTube con posterioridad a su emisión. Pueden revivir la charla y también descargar el PowerPoint usado por Hernán aquí: https://csirt.gob.cl/noticias/charlas-csirt-2023-conceptos-basicos-1/

Si quieren ver las siguientes charlas escríbanos a csirt-comunicaciones@interior.gob.cl y los incluiremos en la lista de distribución de cada videoconferencia.

CSIRT realiza charla telemática "A un clic del desastre", como parte de sus esfuerzos de concientización durante el Mes de la Ciberseguridad

En el marco del Mes de la Ciberseguridad, el equipo del CSIRT de Gobierno participó en una charla virtual llamada "A un clic del desastre", la cual explicó a los trabajadores de BHP los tipos de amenazas, vulnerabilidades, el rol de los trabajadores en la ciberseguridad y las consecuencias de un ciberataque, entre otros temas.

Ciberconsejos | ¿Cómo actuar en caso de ser víctima de phishing?

Correos electrónicos, mensajes de textos o app de mensajería. Distintos son los canales que utilizan los delincuentes para enviar mensajes falsos y así estafar a las personas, con la finalidad de robar los datos de sus cuentas bancarias u otra información personal. En el caso de caer en un phishing, ¿qué se debe hacer?

Revísalo aquí: https://csirt.gob.cl/recomendaciones/ciberconsejos-victima-phishing/

4. 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.

5. 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.

- Diego Ignacio Concha de la Fuente
- Natán Finol Bencomo
- Ítalo Alberto Foppiano Reyes
- Martín Muñoz
- OSI VTI Universidad de Chile
- Milena Mariel Hidalgo Acuña

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.13 16:34:29 -03'00'