CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 238

semana del 19 al 25 de enero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

5

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

6

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

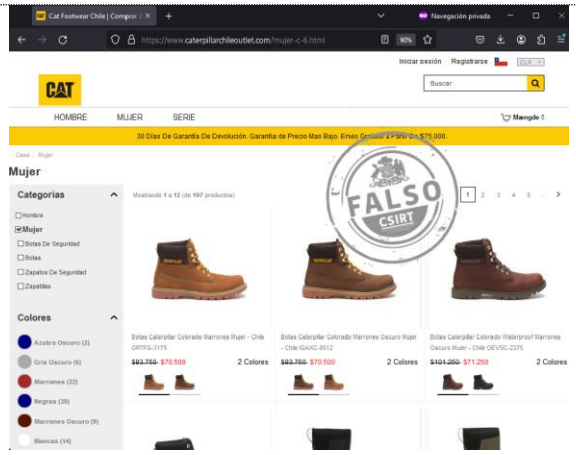
312

Las mitigaciones son útiles en productos de Oracle, Apple, Git Lab, Splunk, TianoCore, Google y Mozilla.

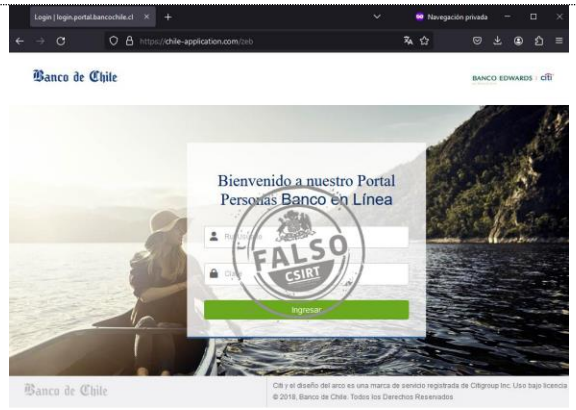
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

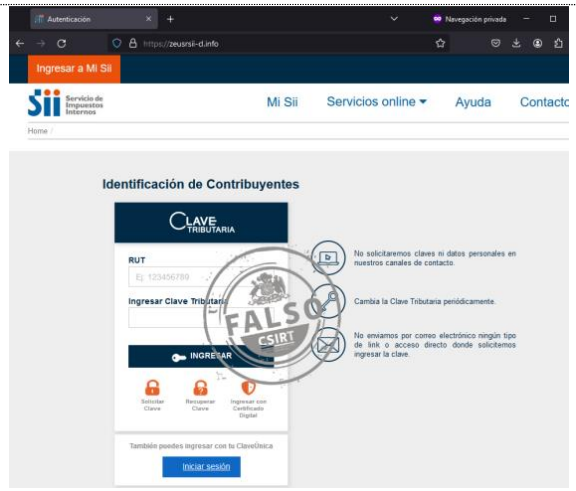
1. Sitios fraudulentos



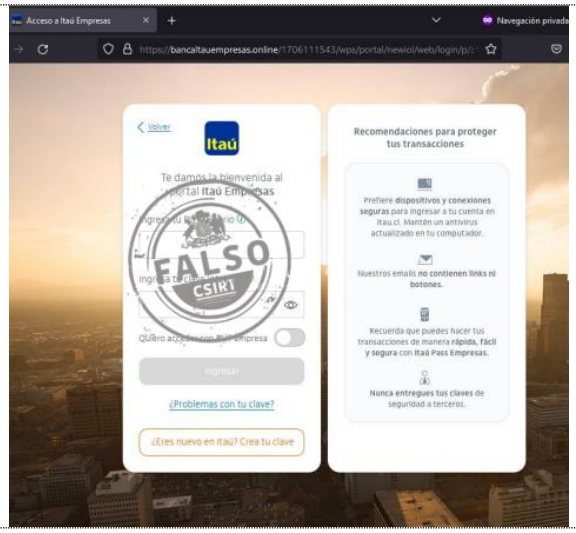
CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01634-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 enero, 2024
Última revisión	19 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.caterpillarchileoutlet[.]com	
URL de redirección	
N/A	
Dirección IP sitio falso	
[172.67.155.226]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01634-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01635-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 enero, 2024
Última revisión	19 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://chile-application[.]com/zeb	
URL de redirección	
N/A	
Dirección IP sitio falso	
[172.67.195.90]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01635-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta al Servicio de Impuestos Internos	
Alerta de seguridad cibernética	8FFR23-01636-01
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://zeusrsii-cl[.]info/	
URL de redirección	
N/A	
Dirección IP sitio falso	
[172.67.205.138]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01636-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Itaú	
Alerta de seguridad cibernética	8FFR23-01637-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 enero, 2024
Última revisión	24 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://bancaltauempresas[.]online/	
URL de redirección	
N/A	
Dirección IP sitio falso	
[51.79.176.23]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01637-01/	

2. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00924-01
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://fogape.theaerie[.]ca/1706111130/imagenes/_personas/home/default.asp	
URL de redirección	
https://maximocontaval[.]com/activacion/cuenta-kaoi/	
Dirección IP sitio falso	
[84.247.167.213]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00924-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas en el Oracle CPU de enero 2024	
Alerta de seguridad cibernética	9VSA24-00960-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 enero, 2024
Última revisión	19 enero, 2024

CVE		
CVE-2023-3823	CVE-2023-31486	CVE-2024-20924
CVE-2019-10086	CVE-2023-31582	CVE-2024-20925
CVE-2020-15250	CVE-2023-32002	CVE-2024-20926
CVE-2020-26870	CVE-2023-32006	CVE-2024-20927
CVE-2020-5410	CVE-2023-32559	CVE-2024-20928
CVE-2020-5421	CVE-2023-32697	CVE-2024-20929
CVE-2020-7760	CVE-2023-33201	CVE-2024-20930
CVE-2021-0341	CVE-2023-34034	CVE-2024-20931
CVE-2021-29425	CVE-2023-34035	CVE-2024-20932
CVE-2021-33813	CVE-2023-34053	CVE-2024-20933
CVE-2021-35515	CVE-2023-34055	CVE-2024-20934
CVE-2021-35516	CVE-2023-34453	CVE-2024-20935
CVE-2021-35517	CVE-2023-34454	CVE-2024-20936
CVE-2021-36090	CVE-2023-34455	CVE-2024-20937
CVE-2021-36090	CVE-2023-3446	CVE-2024-20938
CVE-2021-37533	CVE-2023-34462	CVE-2024-20939
CVE-2021-4104	CVE-2023-34624	CVE-2024-20940
CVE-2021-41182	CVE-2023-34981	CVE-2024-20941
CVE-2021-41183	CVE-2023-35141	CVE-2024-20942
CVE-2021-41184	CVE-2023-35887	CVE-2024-20943
CVE-2021-42392	CVE-2023-36054	CVE-2024-20944
CVE-2021-42575	CVE-2023-3635	CVE-2024-20945
CVE-2021-43306	CVE-2023-36478	CVE-2024-20946
CVE-2021-43527	CVE-2023-36478	CVE-2024-20947
CVE-2021-46848	CVE-2023-36479	CVE-2024-20948
CVE-2022-1471	CVE-2023-36632	CVE-2024-20949
CVE-2022-22950	CVE-2023-37536	CVE-2024-20950
CVE-2022-22969	CVE-2023-3817	CVE-2024-20951
CVE-2022-22979	CVE-2023-3824	CVE-2024-20952
CVE-2022-23221	CVE-2023-38325	CVE-2024-20953
CVE-2022-24839	CVE-2023-38545	CVE-2024-20955
CVE-2022-25147	CVE-2023-38546	CVE-2024-20956
CVE-2022-25647	CVE-2023-39151	CVE-2024-20957
CVE-2022-29155	CVE-2023-39318	CVE-2024-20958
CVE-2022-31147	CVE-2023-39319	CVE-2024-20959
CVE-2022-31160	CVE-2023-39320	CVE-2024-20960
CVE-2022-31690	CVE-2023-39321	CVE-2024-20961
CVE-2022-31692	CVE-2023-39322	CVE-2024-20962
CVE-2022-33879	CVE-2023-39410	CVE-2024-20963
CVE-2022-34169	CVE-2023-39975	CVE-2024-20964
CVE-2022-3479	CVE-2023-40167	CVE-2024-20965
CVE-2022-3510	CVE-2023-41053	CVE-2024-20966

	CVE-2022-3602	CVE-2023-41105	CVE-2024-20967
	CVE-2022-36033	CVE-2023-41900	CVE-2024-20968
	CVE-2022-36944	CVE-2023-42503	CVE-2024-20969
	CVE-2022-37434	CVE-2023-42794	CVE-2024-20970
	CVE-2022-40152	CVE-2023-42795	CVE-2024-20971
	CVE-2022-40896	CVE-2023-43494	CVE-2024-20972
	CVE-2022-41704	CVE-2023-43495	CVE-2024-20973
	CVE-2022-42003	CVE-2023-43496	CVE-2024-20974
	CVE-2022-42004	CVE-2023-43497	CVE-2024-20975
	CVE-2022-42890	CVE-2023-43498	CVE-2024-20976
	CVE-2022-42920	CVE-2023-43622	CVE-2024-20977
	CVE-2022-4304	CVE-2023-43642	CVE-2024-20978
	CVE-2022-4450	CVE-2023-43643	CVE-2024-20979
	CVE-2022-44729	CVE-2023-44483	CVE-2024-20980
	CVE-2022-44730	CVE-2023-44487	CVE-2024-20981
	CVE-2022-45868	CVE-2023-44981	CVE-2024-20982
	CVE-2022-46751	CVE-2023-45143	CVE-2024-20983
	CVE-2022-46908	CVE-2023-45145	CVE-2024-20984
	CVE-2022-48174	CVE-2023-45648	CVE-2024-20985
	CVE-2023-0465	CVE-2023-45802	CVE-2024-20986
	CVE-2023-0466	CVE-2023-46589	CVE-2024-20987
	CVE-2023-1108	CVE-2023-46604	
	CVE-2023-1370	CVE-2023-49093	
	CVE-2023-1436	CVE-2023-4911	
	CVE-2023-20883	CVE-2023-50164	
	CVE-2023-21833	CVE-2023-5072	
	CVE-2023-21901	CVE-2023-5363	
	CVE-2023-21949	CVE-2024-20904	
	CVE-2023-22102	CVE-2024-20905	
	CVE-2023-2283	CVE-2024-20906	
	CVE-2023-23931	CVE-2024-20907	
	CVE-2023-24998	CVE-2024-20908	
	CVE-2023-25194	CVE-2024-20909	
	CVE-2023-2617	CVE-2024-20910	
	CVE-2023-2618	CVE-2024-20911	
	CVE-2023-2650	CVE-2024-20912	
	CVE-2023-27391	CVE-2024-20913	
	CVE-2023-28439	CVE-2024-20914	
	CVE-2023-28484	CVE-2024-20915	
	CVE-2023-28755	CVE-2024-20916	
	CVE-2023-28756	CVE-2024-20917	
	CVE-2023-28823	CVE-2024-20918	
	CVE-2023-29469	CVE-2024-20919	
	CVE-2023-2975	CVE-2024-20920	
	CVE-2023-2976	CVE-2024-20921	
	CVE-2023-30861	CVE-2024-20922	
	CVE-2023-31122	CVE-2024-20923	
	CVE-2023-31484		
	Fabricante		
	Oracle		
	Productos afectados		
	Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers Graph Server and Client Integrated Lights Out Manager (ILOM) JD Edwards EnterpriseOne Orchestrator		

	JD Edwards EnterpriseOne Tools MySQL Cluster MySQL Connectors MySQL Enterprise Monitor MySQL Server MySQL Workbench Oracle Access Manager Oracle Agile PLM Oracle Agile Product Lifecycle Management for Process Oracle Analytics Desktop Oracle Application Object Library Oracle Application Testing Suite Oracle Audit Vault and Database Firewall Oracle Banking APIs Oracle Banking Branch Oracle Banking Cash Management Oracle Banking Collections and Recovery Oracle Banking Corporate Lending Process Management Oracle Banking Credit Facilities Process Management Oracle Banking Digital Experience Oracle Banking Electronic Data Exchange for Corporates Oracle Banking Enterprise Default Management Oracle Banking Extensibility Workbench Oracle Banking Liquidity Management Oracle Banking Origination Oracle Banking Party Management Oracle Banking Supply Chain Finance Oracle Banking Trade Finance Process Management Oracle Banking Virtual Account Management Oracle BI Publisher Oracle Big Data Spatial and Graph Oracle Business Intelligence Enterprise Edition Oracle Business Process Management Suite Oracle Coherence Oracle Commerce Guided Search Oracle Commerce Platform Oracle Common Applications Oracle Communications ASAP Oracle Communications Billing and Revenue Management Oracle Communications BRM – Elastic Charging Engine Oracle Communications Cloud Native Core Automated Test Suite Oracle Communications Cloud Native Core Console Oracle Communications Cloud Native Core Network Data Analytics Function Oracle Communications Cloud Native Core Network Exposure Function Oracle Communications Cloud Native Core Network Function Cloud Native Environment Oracle Communications Cloud Native Core Network Repository Function Oracle Communications Cloud Native Core Network Slice Selection Function Oracle Communications Cloud Native Core Security Edge Protection Proxy Oracle Communications Cloud Native Core Unified Data Repository Oracle Communications Convergence Oracle Communications Convergent Charging Controller Oracle Communications Diameter Signaling Router Oracle Communications Element Manager Oracle Communications Fraud Monitor

	Oracle Communications Instant Messaging Server Oracle Communications IP Service Activator Oracle Communications Messaging Server Oracle Communications MetaSolv Solution Oracle Communications Network Analytics Data Director Oracle Communications Network Charging and Control Oracle Communications Order and Service Management Oracle Communications Policy Management Oracle Communications Pricing Design Center Oracle Communications Service Catalog and Design Oracle Communications Session Report Manager Oracle Communications Unified Assurance Oracle Communications Unified Inventory Management Oracle Complex Maintenance, Repair, and Overhaul Oracle CRM Technical Foundation Oracle Customer Interaction History Oracle Enterprise Data Quality Oracle Enterprise Manager Base Platform Oracle Enterprise Manager for Fusion Middleware Oracle Enterprise Manager for Oracle Database Oracle Enterprise Manager for Oracle Virtual Infrastructure Oracle Enterprise Manager for Virtualization Oracle Enterprise Manager Ops Center Oracle Essbase Oracle Financial Services Analytical Applications Infrastructure Oracle Financial Services Behavior Detection Platform Oracle Financial Services Compliance Studio Oracle Financial Services Enterprise Case Management Oracle Financial Services Lending and Leasing Oracle Financial Services Revenue Management and Billing Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition Oracle FLEXCUBE Enterprise Limits and Collateral Management Oracle FLEXCUBE Investor Servicing Oracle FLEXCUBE Private Banking Oracle Fusion Middleware Oracle GoldenGate Oracle GraalVM for JDK Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle HTTP Server Oracle Hyperion Calculation Manager Oracle Hyperion Financial Data Quality Management, Enterprise Edition Oracle Hyperion Financial Management Oracle Hyperion Financial Reporting Oracle Hyperion Infrastructure Technology Oracle Hyperion Planning Oracle Identity Manager Oracle Installed Base Oracle iStore Oracle iSupport Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle JDeveloper Oracle Knowledge Management Oracle Managed File Transfer Oracle Middleware Common Libraries and Tools

	Oracle NoSQL Database Oracle One-to-One Fulfillment Oracle Outside In Technology Oracle Retail Advanced Inventory Planning Oracle Retail Customer Management and Segmentation Foundation Oracle Retail EFTLink Oracle Service Bus Oracle SOA Suite Oracle Solaris Oracle Utilities Network Management System Oracle Utilties Application Framework Oracle Web Applications Desktop Integrator Oracle WebCenter Content Oracle WebCenter Portal Oracle WebCenter Sites Oracle WebLogic Server Oracle ZFS Storage Appliance Kit PeopleSoft Enterprise PeopleTools Primavera P6 Enterprise Project Portfolio Management Primavera Unifier Siebel CRM
	Enlaces para revisar el informe:
	https://csirt.gob.cl/vulnerabilidades/9vsa24-00960-01/

CSIRT informa de actualizaciones iOS 17.3, iPadOS 17.3 de Apple, que incluyen parches de seguridad		
Alerta de seguridad cibernética	9VSA24-00961-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	23 enero, 2024	
Última revisión	23 enero, 2024	
CVE		
CVE-2024-23212	CVE-2024-23211	CVE-2024-23213
CVE-2024-23218	CVE-2024-23203	CVE-2024-23214
CVE-2024-23208	CVE-2024-23204	CVE-2024-23222
CVE-2024-23207	CVE-2024-23217	CVE-2024-23215
CVE-2024-23223	CVE-2024-23210	CVE-2023-42916
CVE-2024-23219	CVE-2024-23206	CVE-2023-42917
Fabricante		
Apple		
Productos afectados		
iPhone XS y posteriores, iPad Pro 12.9-inch 3ra generación y posteriores, iPad Pro 11-inch 1ra generación y posteriores, iPad Air 3ra generación y posteriores, iPad 8va generación y posteriores, y iPad mini 5ta generación y posteriores.		
Enlaces para revisar el informe:		
https://csirt.gob.cl/vulnerabilidades/9vsa24-00961-01/		

CSIRT comparte información de parche de seguridad contenido en GitLab 16.1.0	
Alerta de seguridad cibernética	9VSA24-00962-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 enero, 2024
Última revisión	23 enero, 2024
CVE	
CVE-2023-7028	
Fabricante	
GitLab Inc.	
Productos afectados	
GitLab Community Edition (CE) y Enterprise Edition (EE) versiones 16.1 a 16.7.1.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00962-01/	

CSIRT informa de nuevas actualizaciones en Splunk, incluyendo una de severidad alta		
Alerta de seguridad cibernética	9VSA24-00963-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	23 enero, 2024	
Última revisión	23 enero, 2024	
CVE		
CVE-2024-23675 CVE-2024-23676	CVE-2024-23677	CVE-2024-23678
Fabricante		
Splunk		
Productos afectados		
Splunk Enterprise for Windows		
Enlaces para revisar el informe:		
https://csirt.gob.cl/vulnerabilidades/9vsa24-00963-01/		

CSIRT informa vulnerabilidades «PixieFAIL» en interfaz UEFI TianoCore EDKII	
Alerta de seguridad cibernética	9VSA24-00964-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 enero, 2024
Última revisión	24 enero, 2024

CVE

CVE-2023-45229	CVE-2023-45233	CVE-2023-45237
CVE-2023-45230	CVE-2023-45234	CVE-2022-36763
CVE-2023-45231	CVE-2023-45235	CVE-2022-36764
CVE-2023-45232	CVE-2023-45236	CVE-2022-36765

Fabricante

TianoCore

Productos afectados

Al menos 23 proveedores afectados (entre ellos, productos de Lenovo, Intel, AMI, Phoenix, Acer, e Insyde).

Enlaces para revisar el informe:

https://csirt.gob.cl/vulnerabilidades/9vsa24-00964-01/

CSIRT comparte información de actualización Google Chrome 121	
Alerta de seguridad cibernética	9VSA24-00965-01
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-2024-0807	CVE-2024-0814	CVE-2024-0804
CVE-2024-0812	CVE-2024-0813	CVE-2024-0811
CVE-2024-0808	CVE-2024-0806	CVE-2024-0809
CVE-2024-0810	CVE-2024-0805	

Fabricante

Google

Productos afectados

Google Chrome, todas las versiones anteriores a 121.0.6167.85 para Mac y Linux y 121.0.6167.85/.86 para Windows.

Enlaces para revisar el informe:

https://csirt.gob.cl/vulnerabilidades/9vsa24-00965-01/

CSIRT comparte información de vulnerabilidades parchadas en Firefox 122		
Alerta de seguridad cibernética	9VSA24-00966-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	25 enero, 2024	
Última revisión	25 enero, 2024	
CVE		
CVE-2024-0741	CVE-2024-0746	CVE-2024-0751
CVE-2024-0742	CVE-2024-0747	CVE-2024-0752
CVE-2024-0743	CVE-2024-0748	CVE-2024-0753
CVE-2024-0744	CVE-2024-0749	CVE-2024-0754
CVE-2024-0745	CVE-2024-0750	CVE-2024-0755
Fabricante		
Mozilla		
Productos afectados		
Firefox, Firefox ESR y Thunderbird.		
Enlaces para revisar el informe:		
https://csirt.gob.cl/vulnerabilidades/9vsa24-00966-01/		

5. Noticias y concientización

Ciberconsejos | Cómo identificar las fake news

Las «fake news» o noticias falsas son informaciones mentirosas, inexactas o engañosas que se difunden principalmente a través de las redes sociales o WhatsApp, y que tienen el objetivo de desinformar o engañar sobre algún tema en particular. Para reconocer un caso de fake news, y así protegerte de la desinformación y no ser culpable de diseminarla, te entregamos los siguientes ciberconsejos: https://csirt.gob.cl/recomendaciones/ciberconsejos-como-identificar-las-fake-news/.

Recueden que siempre los pueden compartir con sus compañeros y trabajadores.

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.

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.

- Ricardo Salas
- Pablo Ignacio Pizarro Cortínez
- Centro Coordinador CSIRT de la Defensa
- David Soto
- Alonso Villalobos González
- Felipe Daniel Gallardo Miranda
- Martín Molina Jarpa
- Jorge Guerra
- Cristian Manuel Balboa Vidal

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.26 17:21:41 -03'00'