



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 235

semana del 29 de diciembre  
de 2023 al 4 de enero de 2024

# LA SEMANA EN CIFRAS

## PARCHES COMPARTIDOS

# 19

Las mitigaciones son útiles en productos de Mozilla, Fortinet y Apache.





# CONTENIDO

1. Vulnerabilidades.....	3
2. Noticias y concientización.....	5
3. Recomendaciones y buenas prácticas .....	6
4. Muro de la Fama .....	7

11111<

## 1. Vulnerabilidades



**INFORME DE Vulnerabilidad**

**9VSA23-00947-01**  
 CSIRT comparte información de una vulnerabilidad día cero en Apache OfBiz

PARA REGISTRAR | 1510  
 UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
 Equipo de Respuesta ante Incidentes de Seguridad Informática

<b>CSIRT alerta de nueva vulnerabilidad día cero en Apache OfBiz</b>	
Alerta de seguridad cibernética	9VSA23-00947-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 enero, 2024
Última revisión	2 enero, 2024
<b>CVE</b>	
CVE-2023-51467	
<b>Fabricante</b>	
Apache	
<b>Productos afectados</b>	
Apache OfBiz, versiones anteriores a la 18.12.11.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://csirt.gob.cl/vulnerabilidades/9vsa23-00947-01/">https://csirt.gob.cl/vulnerabilidades/9vsa23-00947-01/</a>	



**INFORME DE Vulnerabilidad**

**9VSA23-00948-01**  
 CSIRT comparte información de vulnerabilidades parchadas en Firefox 121

PARA REGISTRAR | 1510  
 UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
 Equipo de Respuesta ante Incidentes de Seguridad Informática

<b>CSIRT comparte información de vulnerabilidades parchadas en Firefox 121</b>			
Alerta de seguridad cibernética	9VSA23-00948-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	2 enero, 2024		
Última revisión	2 enero, 2024		
<b>CVE</b>			
CVE-2023-6856	CVE-2023-6859	CVE-2023-6861	CVE-2023-6871
CVE-2023-6135	CVE-2023-6866	CVE-2023-6868	CVE-2023-6863
CVE-2023-6865	CVE-2023-6860	CVE-2023-6869	CVE-2023-6864
CVE-2023-6857	CVE-2023-6867	CVE-2023-6870	CVE-2023-6873
CVE-2023-6858			
<b>Fabricante</b>			
Mozilla			
<b>Productos afectados</b>			
Firefox 120			
Firefox ESR 115.5			
Thunderbird 115.5			
<b>Enlaces para revisar el informe:</b>			
<a href="https://csirt.gob.cl/vulnerabilidades/9vsa23-00948-01/">https://csirt.gob.cl/vulnerabilidades/9vsa23-00948-01/</a>			

### CONTACTO Y REDES SOCIALES CSIRT





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



## CSIRT comparte información de vulnerabilidad en FortiOS, FortiProxy y FortiPAM

Alerta de seguridad cibernética	9VSA23-00949-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 enero, 2024
Última revisión	4 enero, 2024
<b>CVE</b>	
CVE-2023-36639	
<b>Fabricante</b>	
Fortinet	
<b>Productos afectados</b>	
FortiProxy 7.2.0 a 7.2.4 y 7.0.0 a 7.0.10	
FortiOS: 7.4.0, 7.2.0 a 7.2.4 y 7.0.0 a 7.0.11, 6.4.0 a 6.4.12, 6.2.0 a 6.2.15. 6.0.0 a 6.0.17	
FortiPAM: 1.0.0 a 1.0.3	
<b>Enlaces para revisar el informe:</b>	
<a href="https://csirt.gob.cl/vulnerabilidades/9vsa23-00949-01/">https://csirt.gob.cl/vulnerabilidades/9vsa23-00949-01/</a>	

## 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. Noticias y concientización

### Ciberconsejos | Cómo usar un antivirus en tu computador

Un antivirus es un software que busca detectar, prevenir y eliminar programas maliciosos de tu computador. Esta semana, el CSIRT de Gobierno entrega recomendaciones para el uso de este #software en tu computador. Ver también en: <https://csirt.gob.cl/recomendaciones/ciberconsejos-como-usar-un-antivirus-en-tu-computador/>



### ¿Qué es un antivirus?

Software que busca detectar, prevenir y eliminar programas maliciosos de tu computador. Protege tu dispositivo, por ejemplo, revisando las descargas que realizas, los pendrive que conectas y las aplicaciones que usas.







### ¿Qué debes saber?

- Algunos sistemas operativos como Windows cuentan con un antivirus integrado. Asegúrate de que se encuentre activo y actualizado.
- Para una mejor protección, es necesario mantener actualizados los antivirus. Así, tendrás la última información y versión disponible.
- En caso de descargar uno de estos software, hazlo siempre desde el sitio oficial del proveedor.
- Infórmate antes de comprar o descargar un programa sobre sus características y si es adecuado para tu computador.



### CONTACTO Y REDES SOCIALES CSIRT

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



## 3. 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

## 4. 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.

- María José Salas Phishing
- Yang Arguinzones Phishing
- Francisco Jiménez Alcántara Phishing
- Francisco Pons León Phishing
- Marcelo Eduardo Carvajal Vidal Phishing
- Daniella Rodríguez Moral Phishing
- Juan Carlos Muñoz Phishing

### CONTACTO Y REDES SOCIALES CSIRT