



Vulnerabilidad de Día Cero en el sistema ERP de Apache OfBiz expone a las empresas a ataques

Se ha detectado un nuevo fallo de seguridad zero-day en Apache OfBiz, un sistema ERP de código abierto, que podría ser utilizado para saltarse las medidas de autenticación.

Este problema, denominado [CVE-2023-51467](#), afecta a la funcionalidad de inicio de sesión y surgió debido a un parche incompleto que intentaba resolver otro problema crítico ([CVE-2023-49070](#), puntuación CVSS: 9.8) divulgado recientemente.

El equipo de investigación de amenazas SonicWall Capture Labs, quienes identificaron esta vulnerabilidad, [mencionó](#): «El intento de solucionar el CVE-2023-49070 dejó sin resolver el problema raíz, dejando la puerta abierta para saltarse la autenticación».

```
34a
<!-- End Template component://rainbowstone/template/Login.ftl -->
</div><!-- End Section Widget -->

<div class="clear">
</div> </div> </div><!-- Begin Section Widget -->
<!-- Begin Section Widget Render-Footer -->
<!-- Begin Template component://rainbowstone/template/includes/Footer.ftl -->
<div id="footer-offset"></div>
<div id="footer">
  <span>12/19/23, 3:32 AM - <a href="https://sw-ofbiz.local:8443/webtools/control/ListTimezones">Eastern Daylight Time</a></span>
  <span>Copyright (c) 2001-2023
    <a href="http://www.apache.org" target="_blank">The Apache Software Foundation</a>. Powered by
    <a href="http://ofbiz.apache.org" target="_blank">Apache OfBiz.</a> Release
18.12
  </span>
</div>
</div>
<script type="application/javascript" src="//rainbowstone/js/rainbowstone.js"></script>
</body>
</html>

21d
<!-- End Template component://rainbowstone/template/includes/Footer.ftl -->
<!-- End Section Widget Render-Footer -->
<!-- End Section Widget -->
<!-- End Screen component://common-theme/widget/CommonScreens.xml#GlobalDecorator -->
<!-- End Screen component://common/widget/CommonScreens.xml#GlobalDecorator -->
<!-- End Screen component://webtools/widget/CommonScreens.xml#main-decorator -->
<!-- End Screen component://common-theme/widget/CommonScreens.xml#login -->
<!-- End Screen component://common/widget/CommonScreens.xml#login -->

0
sonicwall@sw-2004:~$
```



Vulnerabilidad de Día Cero en el sistema ERP de Apache OfBiz expone a las empresas a ataques

El CVE-2023-49070 es una falla de ejecución remota de código que afecta a versiones anteriores a la 18.12.10. Cuando se explota adecuadamente, permite a los atacantes obtener control total del servidor y acceder a datos confidenciales. Esta vulnerabilidad surge debido a un componente XML-RPC desactualizado en Apache OFBiz.

SonicWall señaló que, utilizando parámetros de USUARIO y CLAVE inválidos o en blanco en una solicitud HTTP, se puede obtener un mensaje de autenticación exitosa, eludiendo así las medidas de seguridad y permitiendo el acceso a recursos internos sin autorización.

El truco de este ataque radica en modificar el parámetro `requirePasswordChange` a «Y» en la URL, lo que facilita eludir la autenticación, sin importar qué datos se ingresen en los campos de usuario y contraseña.

El NIST describió este problema como: *«Esta vulnerabilidad posibilita que los atacantes obvien la autenticación, llevando a cabo una Falsificación de Petición del Servidor (SSRF)»*.

Se aconseja a quienes usen Apache OFbiz que actualicen a la [versión 18.12.11](#) o más reciente lo más pronto posible para reducir riesgos.