

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**ATAQUE A LA CADENA DE SUMINISTRO DE  
ORACLE CLOUD: 6 MILLONES DE REGISTROS  
ROBADOS**

25 / 03 / 2025

## CONTENIDO

INTRODUCCIÓN .....	3
RESUMEN .....	5
CONTACTOS DE SOPORTE .....	7

## INTRODUCCIÓN

En un nuevo golpe a la seguridad en la nube, Oracle Cloud se ha visto envuelto en una posible brecha de seguridad que podría haber expuesto información sensible de más de 140,000 organizaciones. Un ciberdelincuente afirmó en el foro Breach Forums haber robado seis millones de registros de los servicios de autenticación SSO y LDAP de Oracle Cloud, ofreciendo los datos en venta o a cambio de exploits de día cero. Aunque Oracle niega la brecha, expertos en ciberseguridad han identificado un endpoint de producción comprometido que podría validar las afirmaciones del atacante. Esta situación subraya la creciente amenaza de los ataques a la cadena de suministro, donde la explotación de vulnerabilidades en infraestructuras críticas puede afectar a una gran cantidad de empresas de manera simultánea. En este artículo, exploramos los detalles del ataque, su posible impacto y las medidas recomendadas para mitigar riesgos.

## ATAQUE A LA CADENA DE SUMINISTRO DE ORACLE CLOUD: 6 MILLONES DE REGISTROS ROBADOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_02_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	25/03/2025
Es día cero (0 day):	No

## RESUMEN

**Un presunto ciberataque compromete credenciales de SSO y LDAP de Oracle Cloud**

El 20 de marzo de 2025, un usuario del foro de ciberdelincuentes Breach Forums, identificado como “rose87168”, afirmó haber robado seis millones de registros de los servicios SSO y LDAP de Oracle Cloud. El atacante puso a la venta la información o la ofreció a cambio de exploits de día cero. Según la publicación, los datos robados incluyen contraseñas cifradas de SSO y LDAP, archivos Java Keystore (JKS), claves y JPS keys del Enterprise Manager.

Oracle cloud traditional hacked (login.(X).oraclecloud.com)  
by rose87168 - Thursday March 20, 2025 at 02:40 PM

Yesterday, 02:40 PM. (This post was last modified: Yesterday, 02:44 PM by rose87168.)

**rose87168**  
Breach  
MEMBER  
Posts: 2  
Threads: 2  
Joined: Mar 2025  
Reputation: 0

Hello,  
Oracle traditional servers were hacked (domains : login.(region-name).oraclecloud.com )  
Around 6 million user customers' data from SSO and LDAP was stolen.  
JKS files, passwords, key files, and enterprise manager JPS keys were also taken.  
The SSO passwords are encrypted, they can be decrypted with the available files. also LDAP hashed password can be cracked. (I couldn't do it, but if someone can tell me how to decrypt them, I can give them some of the data as a gift.)  
I'll list the domains of all the companies in this leak. Companies can pay a specific amount to remove their employees' information from the list before it's sold.  
I can also trade for 0-day exploits. send me a private message (PM).  
oracle can send me a message through the company's official email to My Email with 72H ( we talk before )  
**PM for Offer**

Sample LDAP > [REDACTED]  
Company list > [REDACTED]  
Sample DataBase > [REDACTED]

```
[align=left]# Matt Wallace, users, 11987096172814988, cloud.oracle.com[/align]
dn: cn=Matt Wallace,cn=users,orclMNTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclntuid: efkd-test.matt.wallace@hitchiner.com
tenantadmin: cn=TenantAdminGroup,cn=Groups,orclMNTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprivilegeuc: cn=orclUserWritePrivilegeGroup,cn=SystemIDGroups,cn=Groups,orclMNTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userreadprivilegeuc: cn=orclUserReadPrivilegeGroup,cn=SystemIDGroups,cn=Groups,orclMNTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprefprivilegeuc: cn=orclUserWritePrefPrivilegeGroup,cn=SystemIDGroups,cn=Groups,orclMNTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclmntenantname: efkd-test
orclmntenantguid: 11987096172814988
orclmntenantstate: ENABLED
authpassword:oid: (SASL/MDS1)UyftNeZlxsfJ6GyfoIsJIw==
authpassword:oid: (SASL/MDS1)X6mV1KALq1Pria0xCM6A==
```

**Posible vector de ataque y vulnerabilidad explotada**

El atacante declaró haber comprometido servidores de Oracle a través de la dirección ‘login.(region-name).oraclecloud.com’ mediante una vulnerabilidad conocida en Oracle Cloud. Aunque no se ha divulgado ninguna prueba de concepto (PoC) pública, se especula que el ataque pudo haber explotado una falla crítica en Oracle Fusion Middleware, posiblemente la [CVE-2021-35587](#).

**Respuesta de Oracle y análisis de expertos**

Oracle negó la brecha de seguridad y aseguró a varios medios de comunicación que no se ha producido pérdida de datos ni compromiso de clientes de Oracle Cloud.

Investigadores analizaron la publicación en Breach Forums y afirmó haber encontrado un endpoint SSO de producción comprometido que respalda la afirmación del atacante. El servidor afectado (login.us2.oraclecloud.com) es un endpoint de producción válido utilizado para autenticación OAuth2 y generación de tokens.

### **Impacto y medidas de mitigación**

El incidente podría afectar a las 140,000 organizaciones listadas en la publicación del atacante y a muchas otras que utilizan soluciones SaaS alojadas en Oracle Cloud. Como medida de precaución, la empresa de ciberseguridad Arctic Wolf recomienda:

- **Restablecer credenciales de Oracle:** Cambiar las contraseñas de SSO y LDAP, así como cualquier otra credencial asociada.
- **Actualizar métodos de autenticación de Oracle:** Regenerar hashes SASL/MD5 o migrar a métodos más seguros.
- **Implementar MFA y políticas de contraseñas robustas:** Refuerza la seguridad de accesos críticos.

Aunque la veracidad de la brecha aún está en investigación, las organizaciones deben actuar con prontitud para mitigar posibles riesgos y reforzar sus estrategias de ciberseguridad.

### **NOTICIA COMPLETA**

<https://devel.group/blog/ataque-a-la-cadena-de-suministro-de-oracle-cloud-seis-millones-de-registros-robados/>



## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto:cert@develsecurity.com)

### Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>