Nro. Alerta:	AL-2025-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	24-mar-2025	Filtración Masiva de Credenciales en Oracle Cloud	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Información
Nivel de riesgo: Alta

II. ALERTA

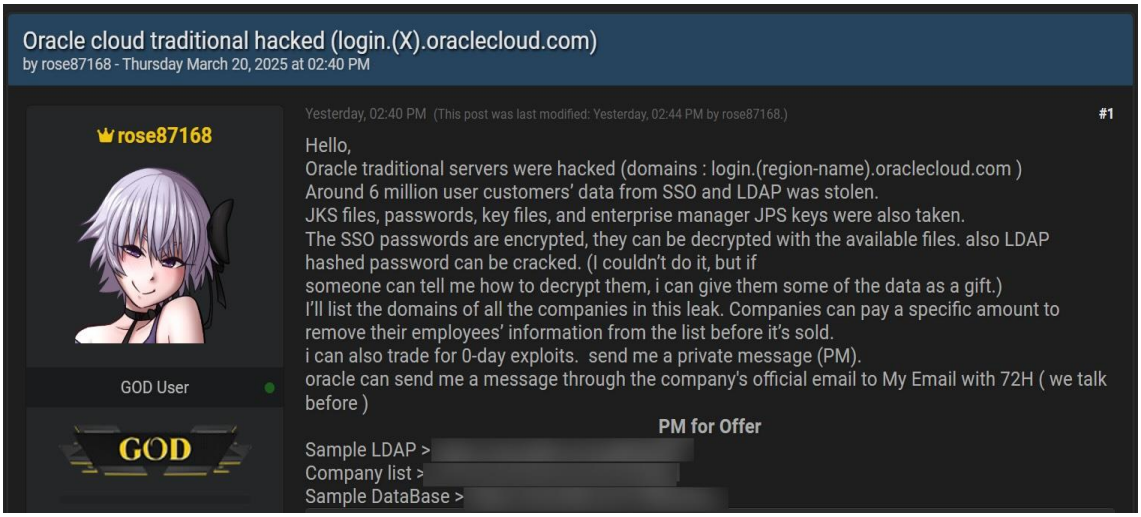

Figura 1.- Foro del atacante - figura referencial

Un atacante de nombre rose87168 afirmo haber robado 6 millones de registros de datos de los sistemas de autenticación de Oracle Cloud, SSO (Oracle Single Sign-On) y LDAP (Lightweight Directory Access Protocol).

III. INTRODUCCIÓN

El atacante anuncio los supuestos registros robados en un foro de la dark web y que afectaría a 140.000 inquilinos, entre los datos comprometidos están:

- Contraseñas SSO cifradas, que son utilizado para un solo inicio de sesión; pueden permitir un acceso no autorizado.
- Contraseñas LDAP cifradas, son usadas para autenticación de directorios; puede permitir un acceso no autorizado.
- Archivos JKS (Java Key Store), almacenan claves y certificados criptográficos para aplicaciones Java.
- Claves JPS (Java Platform Security), sirven para administrar el acceso y el cifrado en Oracle Enterprise Manager.

El atacante no tan solo con exigir a las organizaciones que paguen para no exponer los datos de sus registros y de extorsionar económicamente a Oracle para proveer información sobre como vulnero el acceso a sus servidores, también ofrece un incentivo a cualquiera que le ayudara a descifrar las contraseñas SSO y/o crackear contraseñas LDAP.

IV. VECTOR DE ATAQUE

El atacante afirmó haber comprometido una versión vulnerable de los servidores de Oracle Cloud (en el subdominio login.us2.oraclecloud.com) mediante un CVE público (fallo), que actualmente no tiene PoC (Proof of Concept) o exploit público. Incluso compartió una imagen con información que demuestra el acceso al servidor de Oracle, incluyendo la carga de un archivo txt con la dirección de su correo electrónico en el dominio de inicio de sesión.

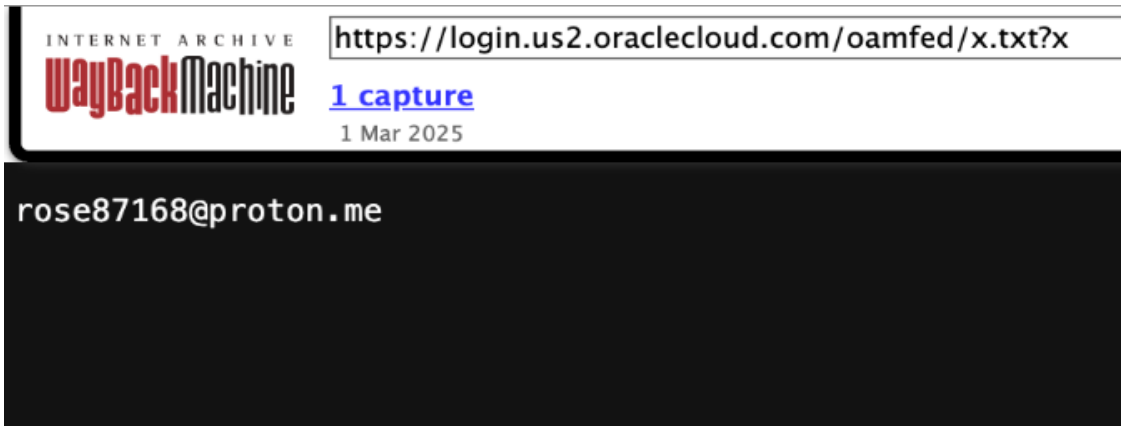

Figura 2.- La explotación del subdominio de Oracle Cloud en la región US2.

Dado lo mencionado por el atacante, las investigaciones del subdominio login.us2.oraclecloud.com indican que este alberga el servidor de Oracle Fusion Middleware, un servidor que no recibe actualizaciones desde el 27 de septiembre del 2014.

Figura 3.- Servidor Oracle Fusion Middleware en el subdominio de Oracle Cloud.

Figura 4.- Última actualización de Oracle Fusion Middleware

El servidor de Fusion Middleware tenía una vulnerabilidad crítica denominada CVE-2021-35587 que afecta a Oracle Access Manager (OpenSSO Agent) en las versiones:

- 11.1.2.3.0
- 12.2.1.3.0
- 12.2.1.4.0

Esta vulnerabilidad fácilmente explotable permite a un atacante no autentificado con acceso a la red a través de HTTP comprometer a Oracle Access Manager. La explotación exitosa puede conducir a una toma completa de Oracle Access Manager.

V. IMPACTO

Exposición de datos masivos: El compromiso de 6 millones de registros, que incluyen datos sensibles relacionados con la autenticación, aumenta los riesgos de acceso no autorizado y espionaje corporativo.

Credenciales comprometidas: Contraseñas cifradas de SSO y LDAP, si se crackean, podrían permitir nuevas brechas en entornos de Oracle Cloud.

Extorsión y demandas de rescate: El atacante está presionando a las empresas afectadas para que paguen por la eliminación de los datos, lo que aumenta los riesgos financieros y de reputación.

Explotación del Día Cero: El presunto uso de una vulnerabilidad de día cero genera preocupación sobre la seguridad de Oracle Cloud y posibles ataques futuros.

Riesgos de la Cadena de Suministro: La exposición de archivos JKS y de claves podría permitir a los atacantes moverse lateralmente y comprometer múltiples sistemas empresariales interconectados.

VI. RECOMENDACIONES:

- **Restablecer contraseñas:** Cambia todas las contraseñas LDAP comprometidas, priorizando cuentas con privilegios. Aplica MFA y políticas seguras.
- **Actualizar autenticación:** Regenera hashes SASL/MD5 o migra a métodos más seguros.
- **Rotar credenciales de inquilino:** Contacta a Oracle para actualizar identificadores específicos.
- **Reemplazar certificados y secretos:** Sustituye credenciales SSO/SAML/OIDC afectadas.
- **Auditoría y monitoreo:** Revisa registros LDAP, investiga actividad sospechosa y habilita monitoreo continuo.
- **Refuerzo de seguridad:** Rota credenciales, analiza incidentes, monitorea amenazas y reporta a Oracle.
- **Fortalecer controles de acceso:** Aplica el mínimo privilegio y mejora registros para detectar anomalías.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants

https://orca.security/resources/blog/oracle-cloud-breach-exploiting-cve-2021-35587/

https://www.cvedetails.com/cve/CVE-2021-35587/

https://www.bleepingcomputer.com/news/security/oracle-denies-data-breach-after-hacker-claims-theft-of-6-million-data-records/

https://www.kippel01.com/tecnologia/oracle-asegura-hubo-brecha-seguridad-tras-las-afirmaciones-hacker-6-millones-registros-robados

https://research.kudelskisecurity.com/2025/03/21/oracle-cloud-sso-ldap-records-dumped-140k-tenants-affected/

https://hackread.com/oracle-denies-breach-hacker-access-6-million-records/