CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 24/03/2025

Type de Contenu	Description
Titre	***Fuite de données présumées d'Oracle Cloud revendiquée et mises en vente par un acteur malveillant***
ID	*202503/AS/16*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***Single Sign-On (SSO)*** *et* ***Lightweight Directory Access Protocol (LDAP)*** *d'Oracle.*
Version / Edition	*N/A*
Plateforme	***Oracle Cloud***
Mise à jour	*N/A.*
Résumé	*Un acteur de la menace revendique et met en vente les données de plus de six (06) millions d'utilisateurs présumés d'oracle cloud.*
Impacts	• **Exploitation des identifiants de connexion** • **Compromission des accès : Accès non autorisé à plusieurs systèmes avec un seul identifiant** • **Mouvement latéral & escalade de privilèges : Accès aux comptes à hauts privilèges** • **Fuite de données sensibles : Vol de données clients, financières.**
Description Détaillée	*Un message posté par un acteur de la menace sur un forum* ***clandestin - breachforums[.st]*** *- fait état d'une fuite de données affectant les serveurs d'Oracle. La faille aurait compromis environ* ***six millions d'enregistrements d'utilisateurs****, y compris des données provenant des services* ***Single Sign-On (SSO) et Lightweight Directory Access (LDAP) d'Oracle****. Les informations qui auraient fuité comprennent des fichiers JKS, des fichiers clés, des mots de passe SSO chiffrés, des Hashs de mots de passe LDAP et des clés JPS provenant de l'Enterprise Manager d'Oracle. Certains enregistrements comportent des adresses mails avec plus de* ***140 620*** *domaines.* *L'acteur de la menace offre l'accès à ces données et affirme que les entreprises touchées par la violation peuvent payer pour que les informations concernant leurs employés soient retirées de la liste avant qu'elles ne soient vendues sur le Dark Web et autres forums de vente.* *Comme preuve supplémentaire de ses affirmations, l'acteur de la menace a partagé une* ***URL Wayback Machine*** *pour un fichier* ***.txt*** *sur* ***login.us2.oraclecloud.com****, qui affiche son adresse e-mail ProtonMail.*

	Un échantillon de base de données, une liste des organisations affectées et un échantillon de fichier LDAP ont également été mis en ligne sur un site de partage de fichiers pour vérification. ***Oracle a démenti ces allégations en déclarant : « Il n'y a pas eu de violation d'Oracle Cloud. Les informations d'identification publiées ne concernent pas Oracle Cloud. Aucun client d'Oracle Cloud n'a été victime d'une violation ou n'a perdu de données ».*** *Sur la base de l'analyse de l'échantillon de données et de la présence d'éléments liés à Oracle, il existe des indications d'un accès ou d'une exposition limitée. Bien que l'impact global et la portée restent flous, il serait prudent pour les organisations utilisant les services d'Oracle de revoir leur posture de sécurité par mesure de précaution.* ***L'acteur affirme avoir exploitée une vulnérabilité (CVE) sur des serveurs Oracle Cloud pour exfiltrer les données fuitées. Ainsi, le serveur login.us2.oraclecloud.com était vulnérable à la vulnérabilité CVE-2021-35587, une faille critique (score CVSS de 9,8) connue dans Oracle Access Manager de Fusion Middleware, et plus particulièrement dans son agent OpenSSO. L'exploitation de cette vulnérabilité peut se faire via HTTP sans authentification***
Recommandations	*À la suite de cette violation présumée, il est recommandé aux organisations de prendre les mesures suivantes :* - *Évaluer l'impact potentiel sur les partenaires et les intégrations liées aux services Oracle.* - *Activer l'authentification multifactorielle (MFA) sur le SSO.* - *Vérifier toute activité inhabituelle dans les systèmes connectés à Oracle SSO et LDAP.* - *Contacter l'équipe de sécurité d'Oracle pour obtenir des informations et des conseils supplémentaires en cas de doute.* - *Mettre urgemment à jours les solutions d'Oracle* - *Signaler sur https://cert.tg/ toute activité avérée de fuite de données*
Indicateurs de Compromission	*Acteur de la menace* • *Nom : **rose87168*** • *Email : **rose87168[@]proton[.]me.*** • *Compte X : **@rose87168*** *http://login.us2.oraclecloud.com/oamfed/x.txt?x*
Liens pour plus de détails	*https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants*

USR_KEY	ACT_KEY	USR_LAST_NAME	USR_FIRST_NAME	USR_MIDDLE_NAME	USR_DISPLAY_NAME	USR_MANAGER	USR_TYPE	USR_LOCATION	USR_FSS	USR_TODO	USR_PASSWORD
5023117	1	valakonda	canary	null	tasc		End-User Administrator	null	null	null	
5023207	1	Lim	Mitchell	null	Mitc		End-User	null	null	null	9808:zJcsRsJTD+skAE9U
5023385	1	DAS	PRITISH	null	PRI		End-User	null	null	null	0484:R0c5kIAMT2UvUM9

```
1   USR_LAST_NAME U          AME USR_EMAIL
2   Shin 'Hyunwoo '          in@dhl.com
3   'Ong 'Jake 'jak          com
4   'Asling 'Jan 'j          dhl.com
5   'Sumida 'Akiko           ida@dhl.com
6   'Yang 'Alisa 'a          ng@dhl.com
7   'Kim 'Boryung '          m@dhl.com
8   'Khanthaviti 'C          harunee.khanthaviti@dhl.com
9   'Bui 'Ha 'ha.bu
10  'Wong 'Ivy 'ivy          .com
11  'Burton 'James           ton2@dhl.com
12  'Yeo 'Joana 'jo          l.com
```

```
dn: cn=Patrick Doc          uid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclmtuid: efkd-te          r.com
tenantadmin: cn=Te          orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprivilege          legeGroup,cn=SystemIDGroups,cn=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userreadprivilegeu          egeGroup,cn=SystemIDGroups,cn=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprefspriv          PrefsPrivilegeGroup,cn=SystemIDGroups,cn=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclmttenantuname:
orclmttenantguid:
orclmttenantstate:
authpassword;oid:           T3FCHmg==
authpassword;oid:           HtO0OS8U9g==
authpassword;oid:           lQhJu4ToA==
userpassword:: xxx          xxxxxxxxxxxxxxxxxxxxxxxxxx
objectclass: orcl
objectclass: obli
objectclass: obli
objectclass: OIMPe
objectclass: inetO
objectclass: top
objectclass: organ
objectclass: perso
oblogintrycount: 0
displayname: Patri
cn: Patrick Dodd
employeetype: OTHE
uid: patrick_dodd
obpasswordchangef
mail: patrick_dodd
sn: Dodd
obpasswordexpiryd
givenname: Patrick
```

Figure 1: Quelques echantillons de fuites divulguées et mises en vente par l'acteur