



KPMG Cyber Threat Intelligence Platform

Flash Advisory – Oracle Cloud Supply Chain Attack

CVE Identified : CVE-2021-35587

Base Score : 9.8 Critical

TLP : Clear

KPMG. Make the Difference.



On 20 March 2025, a leak post surfaced involving an alleged breach of Oracle's Cloud authentication. The threat actor claimed to have stolen 6 million records from over 140,000 Oracle Cloud tenants by leveraging a critical vulnerability in Oracle Access Manager, a product of Oracle Fusion Middleware. Despite Oracle denying claims of any breach, the threat actor posted sample data in an attempt to extort ransom from potentially impacted organizations.

The threat actor, tracked by their username as "rose87168", purportedly exploited a vulnerability in Oracle Cloud's authentication system by targeting the EM2 and US2 instances of endpoint "login.(region-name).oraclecloud[.]com". The threat actor also shared an Internet Archive URL indicating that they uploaded a .txt file containing their ProtonMail email address to the impacted instance. The endpoint, which has since been taken down, was observed to be last updated in 2014 and may have been susceptible to CVE-2021-35587. This vulnerability in Oracle Fusion Middleware allows unauthenticated attackers with network access via HTTP to completely compromise Oracle Access Manager (OAM). By exploiting this flaw, the threat actor claimed to have exfiltrated sensitive authentication data, including Java KeyStore (JKS) files, encrypted Single Sign-On (SSO) passwords, hashed Lightweight Directory Access (LDAP) passwords, key files, and Enterprise Manager JPS keys. The stolen data was advertised on hacker forums along with a list of impacted domains, demanding ransom payments to prevent further data exposure. The threat actor is also encouraging third parties to help decrypting the encrypted credentials, amplifying the potential impact and leading to further downstream attacks.

What should you do?

- Enforce password reset for all Oracle Cloud SSO/LDAP users, prioritizing privileged accounts and tenant admins.
- Rotate credentials and replace cryptographic keys and certificates for Oracle environments. Implement strong password policies and enforce MFA.
- Ensure that all Oracle related components are updated with the latest patches.
- Implement continuous monitoring and enhance logging to identify anomalous activities and unusual logins.
- Report to Oracle for official guidance and mitigations.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:

Strategic threat intelligence report

Machine ingestible threat intelligence feeds

Threat intelligence driven pre-emptive threat hunting exercise

Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabbv@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mttembhurkar@kpmg.com

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.



The image shows a screenshot of a forum thread. At the top, the title "Oracle cloud traditional hacked (login(X).oraclecloud.com)" is displayed in white text on a dark blue background, followed by the author's name "by rose87168 - Thursday March 20, 2025 at 02:40 PM". The main content area has a light gray background. On the left side, there is a vertical sidebar containing the user's profile information: a profile picture of a character with purple hair, the username "rose87168" with a crown icon, the title "GOD User", a "GOD" rank badge, and statistics showing 10 posts, 2 threads, joined in Mar 2025, and a reputation of 30. The main body of the post starts with a timestamp "03-20-2025, 02:40 PM" and a note about the last modification. The text begins with "Hello," followed by a paragraph stating that Oracle traditional servers were hacked, listing domains like login.(region-name).oraclecloud.com, and mentioning that around 6 million user customers' data from SSO and LDAP was stolen, along with JKS files, passwords, key files, and enterprise manager JPS keys. A second paragraph says "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. oracle can send me a message through the company's official email to My Email with 72H (we talk before)". Below this are three numbered points: "1- only send offers. (add price in title)", "2- only full data , no single company.", and "3- decryption is not crack service !". Further down, there are three links: "Sample LDAP > https://anonfile.io/f/sgRKh9HJ", "Company list > https://anonfile.io/f/KUJuSgIX", and "Sample DataBase > https://anonfile.io/f/1N4UXKtv". At the bottom, a code block contains a detailed LDAP entry for Matt Wallace, including fields like dn, cn, orclmttenantid, orclmtenantstate, authpassword, objectclass, oblogintycount, displayName, cn, employeetype, and uid.



👑 rose87168



GOD User

GOD

Posts: 10
 Threads: 2
 Joined: Mar 2025
 Reputation: 30

Company list > <https://anonfile.io/f/KUJuSgIX>
Sample DataBase > <https://anonfile.io/f/1N4UXKtv>

```
cn=cmoocm, cn=cmoocm, ou=cmoocm, dc=com
dc=cloud, dc=oracle, dc=com
userwriteprivilege: cn=orclUserWritePrivilegeGroup, cn=SystemIDGroups, cn=Groups, orclMTenantGuid=1987096172814988, dc=cloud, dc=oracle, dc=com
errorreadprivilege: cn=orclUserReadPrivilegeGroup, cn=SystemIDGroups, cn=Groups, orclMTenantGuid=1987096172814988, dc=cloud, dc=oracle, dc=com
userwriteprefsprivilege: cn=orclUserWritePrefsPrivilegeGroup, cn=SystemIDGroups, cn=Groups, orclMTenantGuid=1987096172814988, dc=cloud, dc=oracle, dc=com
orclmttenantname: efkd-test
orclmttenantguid: 11987096172814988
orclmttenantstate: ENABLED
authpasswd;oid: {SASL/MDS}UyfTnsZxsfj6dyfoIsJIw==
authpasswd;oid: {SASL/MDS-DN}jX6mxVjXALq1Px4a0xOWMA==
authpasswd;oid: {SASL/MDS-UJv+XK5sQgdO1E7RZYDCfw==
userpasswd:: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
=
objectclass: orclIDXPerson
objectclass: oblixPersonPwdPolicy
objectclass: oblixOrgPerson
objectclass: OIMPersonPwdPolicy
objectclass: inetorgperson
objectclass: top
objectclass: organizationalPerson
objectclass: person
oblogintycount: 0
displayName: Matt Wallace
cn: Matt Wallace
employeeType: OTHER
uid: matt_wallace@hitchiner.com
obpasswdchangeFlag: true
mail: matt.wallace@hitchiner.com
sn: Wallace
obpasswdexpirydate: 2018-05-24T00:00:00Z
[align=left]givenName: Matt[align]
```

```

[align=left]USR_KEY_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 USR_DISABLED USR_PMD_CANT_CHANGE
USR_PMD_MUST_CHANGE USR_PMD_NEVER_EXPIRES USR_UPDATE_AD_CREATED USR_STATUS USR_EMP_TYPE USR_LOGIN USR_DISABLED BY PARENT USR_PMD_EXPIRE_DATE USR_PMD_WARN_DATE USR_MANAGER_KEY USR_POLICY_UPDATE
USR_PMD_WARNED USR_PMD_EXPIRED USR_START_DATE USR_END_DATE USR_PROVISIONING_DATE USR_DEPROVISIONING_DATE USR_PROVISIONED_DATE USR_DEPROVISIONED_DATE USR_EMAIL USR_LOCKED USR_LOGIN_ATTEMPTS_CTR
USR_PMD_RESET_ATTEMPTS_CTR USR_CHANGE_PMD_AT_NEXT_LOGIN USR_PMD_MIN_AGE DATE USR_DATA_LEVEL USR_CREATE USR_CREATEBY USR_UPDATE USR_UPDATEBY USR_NOTE USR_TIMEZONE USR_LOCALTIME USR_LOCKED_ON
USR_MANUALLY_LOCKED USR_AUTOMATICALLY_DELETE ON USR_FULL_NAME USR_COUNTRY USR_DEPT NO USR_DESCRIPTION USR_COMMON_NAME USR_EMP_NO USR_FAX USR_GEN_QUALIFIER USR_HIRE_DATE USR_HOME_PHONE
USR_LOCALITY_NAME USR_MOBILE USR_PAGER USR_HOME_POSTAL_ADDRESS USR_POSTAL_ADDRESS USR_POSTAL_CODE USR_PO_BOX USR_STATE USR_STREET USR_TELEPHONE_NUMBER USR_TITLE USR_INITIALS USR_PMD_GENERATED
USR_LDAP_ORGANIZATION USR_LDAP_ORGANIZATION_UNIT USR_LDAP_GUID USR_LDAP_ID USR_ROWNER USR_ACCESSIBILITY_MODE USR_COLOR CONTRAST USR_FONT_SIZE USR_NUMBER_FORMAT USR_CURRENCY USR_DATE_FORMAT
USR_TIME_FORMAT USR_EMBEDDED_HELP USR_LANGUAGE USR_TERRITORY USR_NAME_PREFERRED LANG USR_UOF_TENANT_GUID USR_UOF_TENANT_NAME USR_UOF_NOWAIT_LOGIN USR_UOF_EXTERNAL_USER_TYPE USR_UOF_FA_USER_ID
USR_UOF_FA_PERSON_ID USR_UOF_FA_PARTY_ID USR_CN_GENERATED USR_SUMMARY_RISK USR_HAS_HIGH_RISK_ROLE USR_HAS_HIGH_RISK_RESOURCE USR_HAS_HIGH_RISK_ENTITLEMENT USR_HAS_HIGH_RISK_PROV_METH
USR_HAS_HIGH_RISK_OPEN_SDO USR_HAS_HIGH_RISK_LAST_CERT USR_ROLE_SUMMARY_RISK USR_ACCOUNT_SUMMARY_RISK USR_ENTITLEMENT_SUMMARY_RISK USR_RISK_UPDATE_DATE USR_JOB_CODE USR_OFFICE_NAME IS_USR_FEDERATED
[/align]

```

[illegible]