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

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

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

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

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

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

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.

Oracle cloud traditional hacked (login.(X).oraclecloud.com)

by rose87168 - Thursday March 20, 2025 at 02:40 PM

rose87168

GOD User

GOD

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

03-20-2025, 02:40 PM (This post was last modified: Yesterday, 12:14 PM by rose87168. *Edit Reason: add rules*)

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.

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)

1- only send offers. (add price in title)
2- only full data , no single company.
3- decryption is not crack service !

Sample LDAP > **https://anonfile.io/f/sgRKh9HJ**
Company list > **https://anonfile.io/f/KUJuSgIX**
Sample DataBase > **https://anonfile.io/f/1N4UXKtv**

```
[align=left]# Matt Wallace, users, 11987096172814988, cloud.oracle.com[/align]
dn: cn=Matt Wallace,cn=users,orclMTTenantGuid=11987096172814988,dc=cloud,dc=or
acle,dc=com
orclmtuid: efkd-test.matt_wallace@hitchiner.com
tenantadmin: cn=TenantAdminGroup,cn=Groups,orclMTTenantGuid=11987096172814988,
dc=cloud,dc=oracle,dc=com
userwriteprivilegeuc: cn=orclUserWritePrivilegeGroup,cn=SystemIDGroups,cn=Grou
ps,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userreadprivilegeuc: cn=orclUserReadPrivilegeGroup,cn=SystemIDGroups,cn=Groups
,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprefsprivilegeuc: cn=orclUserWritePrefsPrivilegeGroup,cn=SystemIDGrou
ps,cn=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclmttenantuname: efkd-test
orclmttenantguid: 11987096172814988
orclmttenantstate: ENABLED
authpassword;oid: {SASL/MD5}UyfTnsZlxsfJ6Gyfo1sJIw==
authpassword;oid: {SASL/MD5-DN}jX6mxVjXALq1Px4a0xOWWA==
authpassword;oid: {SASL/MD5-U}V+XK5sQjGdO1E7RZNYDCfw==
userpassword:: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
=
objectclass: orclIDXPerson
objectclass: oblixPersonPwdPolicy
objectclass: oblixOrgPerson
objectclass: OIMPersonPwdPolicy
objectclass: inetorgperson
objectclass: top
objectclass: organizationalPerson
objectclass: person
oblogintrycount: 0
displayname: Matt Wallace
cn: Matt Wallace
employeetype: OTHER
uid: matt_wallace@hitchiner.com
```

Follow us on:
kpmg.com/in/socialmedia

KPMG

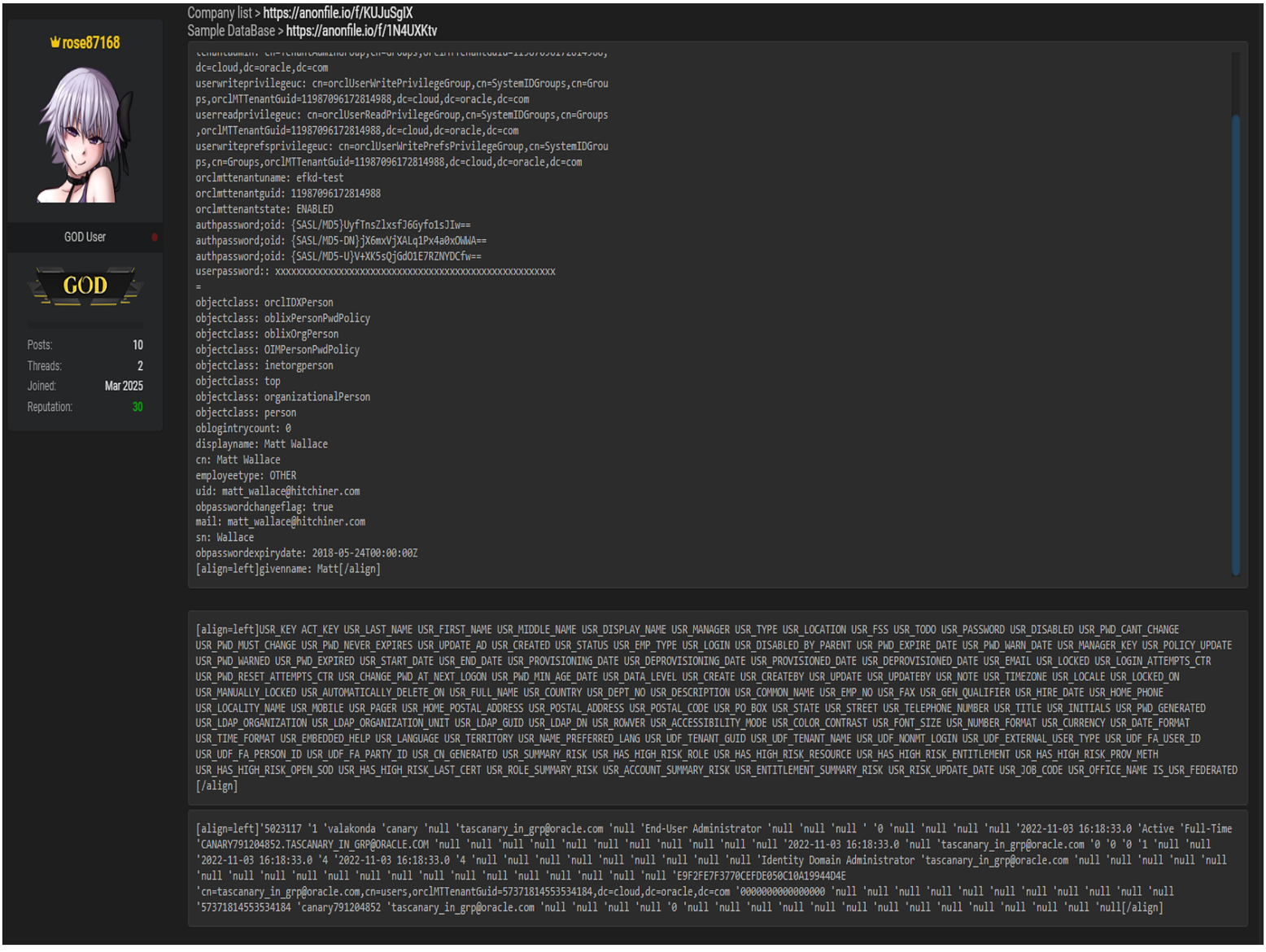
KPMG Cyber Threat Intelligence Platform

Flash Advisory – Oracle Cloud Supply Chain Attack

CVE Identified : CVE-2021-35587 **Base Score : 9.8 Critical**

TLP : Clear

KPMG. Make the Difference.



Follow us on:
kpmg.com/in/socialmedia