

Oracle Cloud Breach

Report by Secutec



Secutec

Cybersecurity Intelligence

Index

1. Executive Summary	2
2. Information from the post	2
3. Analysis	3
4. Critical Vulnerability	4
5. Impact of the Breach	4
6. Mitigation Actions	5
6.1. Audit and Activity Log Review	6
6.1.1. Monitor Audit Logs for Suspicious Activity	6
6.1.2. Set Up Continuous Monitoring & Alerts	7
7. Articles	7
8. Data	8

Change Log

24/03/2025:

The first version of the document has been created.

25/03/2025:

The Threat Actor has now shared a 10,000-line sample to further substantiate their claims. CloudSEK's analysis of this dataset has revealed several critical insights:

- **Wide Impact Across Organisations:** The sample contains data from over 1,500 unique organizations, highlighting the significant scale of the breach.
- **Authenticity of the Data:** The volume and structure of the leaked information make it extremely difficult to fabricate, reinforcing the credibility of the breach.
- **Production Access Indicators:** Many affected organizations have tenantIDs in the format {tenant}-dev, {tenant}-test, and {tenant}, strongly suggesting that the threat actor has access to production environments as well.
- **Exposure of Personal Emails:** The dataset includes a substantial number of personal email addresses, likely resulting from organizations enabling SSO-based authentication for users and customers.
- **Ongoing Validation Efforts:** [Independent researchers](#) who also received this file from the threat actor were able to verify the validity of the leak and confirm that it is indeed a legitimate breach.

CloudSEK will continue to monitor the situation and provide further updates as they gather more intelligence.

26/03/2025:

Updated Mitigation Actions: Immediate Security Measures

Updated Audit and Activity Log Review

Oracle Cloud Breach

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

1. Executive Summary

On March 21, 2025, cybersecurity firm CloudSEK's X Vigil uncovered a major supply chain breach involving Oracle Cloud. A threat actor known as "rose87168" is reportedly selling 6 million records stolen from Oracle's SSO and LDAP systems. The leaked data includes: JKS files, encrypted SSO passwords, key files and enterprise Manager JPS keys.

This attacker has been active since January 2025 and is not just selling the data but also offering decryption assistance - a clear attempt to monetize the breach further. They're even demanding payments from affected organizations to remove their stolen data.

From CloudSEK engagement with the threat actor, it appears that an undisclosed vulnerability in Oracle Cloud's login.(region-name).oraclecloud.com may have been exploited to gain unauthorized access.

While this attacker has no prior history, their techniques suggest a high level of sophistication. CloudSEK has assessed this threat with medium confidence but has rated it as High in severity due to the scale and potential impact on over 140,000 Oracle Cloud tenants.

Check your exposure here - <https://exposure.cloudsek.com/oracle>

2. Information from the post

A threat actor is claiming to have exfiltrated 6 million records from Oracle Cloud and is now listing them on the Dark Web.

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

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

rose87168



Breached

MEMBER

Posts: 2

Threads: 2

Joined: Mar 2025

Reputation: 0

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

#1

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 >
Company list >
Sample DataBase >

```
[align=left]# Matt Wallace, users, 11987096172814988, cloud.oracle.com[/align]
dn: cn=Matt Wallace,cn=users,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,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=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userreadprivilegeuc: cn=orclUserReadPrivilegeGroup,cn=SystemIDGroups,cn=Groups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
userwriteprefprivilegeuc: cn=orclUserWritePrefPrivilegeGroup,cn=SystemIDGroups,orclMTTenantGuid=11987096172814988,dc=cloud,dc=oracle,dc=com
orclmttenantname: efkd-test
orclmttenantguid: 11987096172814988
orclmttenantstate: ENABLED
authpassword;oid: {SASL/MD5}UyfTnsZlxstJ6GyfoIsJlw==
authpassword;oid: {SASL/MD5-DN}iX6mxViXALq1Px4a0x0WNA==
```

The stolen database consists of approximately 6 million records extracted from Oracle Cloud's SSO and LDAP systems, which include:

- JKS files
- Encrypted SSO passwords
- Key files
- Enterprise Manager JPS keys

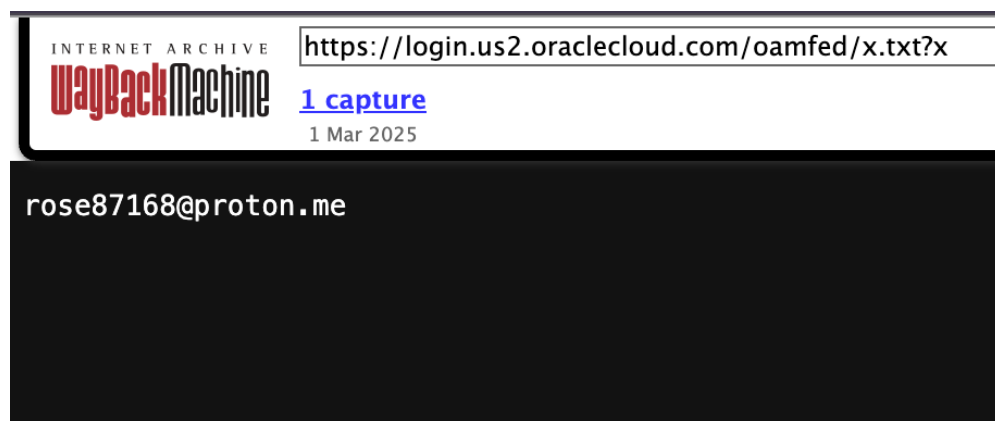
In a bid to further monetize the breach, the threat actor is offering an incentive to anyone who can help decrypt the SSO passwords or crack the LDAP passwords.

The breach affects over 140,000 Oracle Cloud tenants, and the attacker is demanding a "fee" from companies to have their stolen data removed.

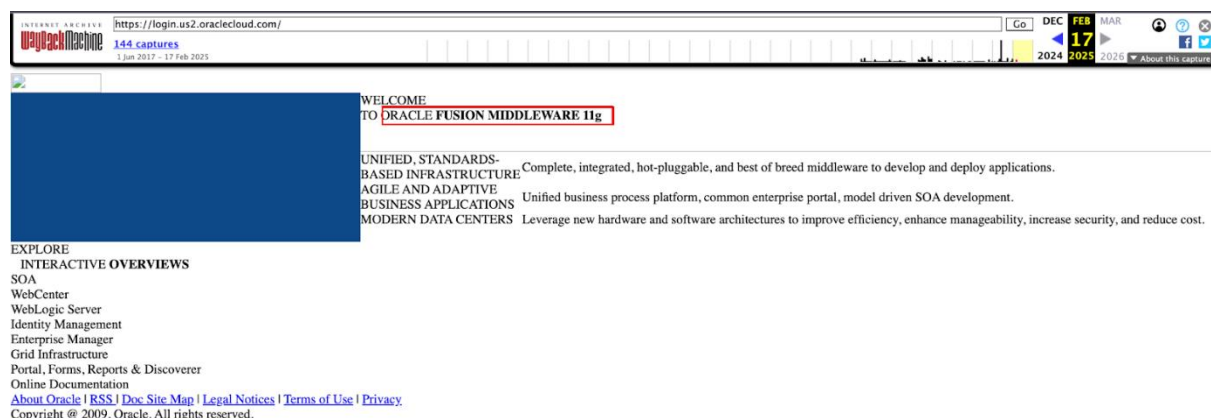
To further their agenda, the threat actor has also created a new X page, where they've begun following Oracle-related pages.

3. Analysis

The threat actor claims to have compromised the subdomain login.us2.oraclecloud.com, which has reportedly been taken down since the breach occurred.



The subdomain was captured on the Wayback Machine on February 17, 2025, suggesting it was hosting Oracle Fusion Middleware 11G at the time.



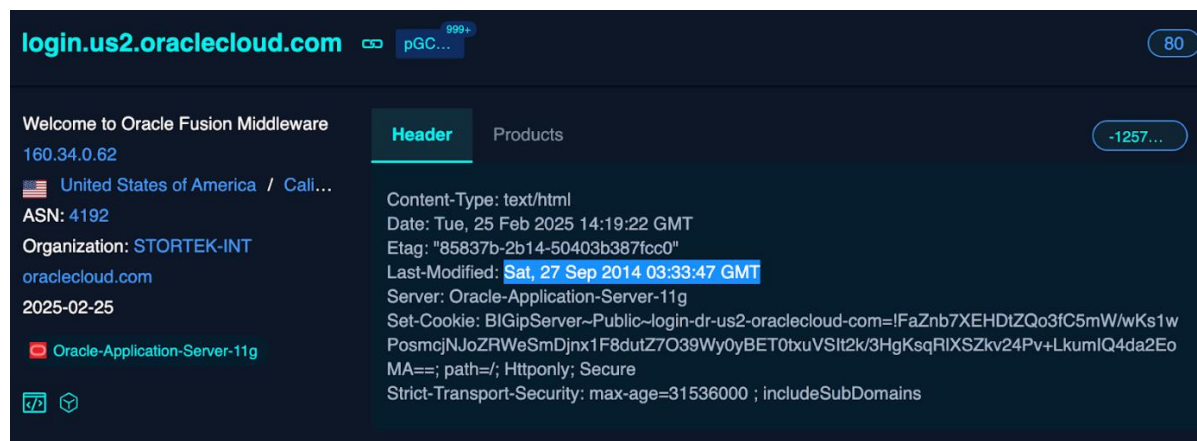
According to FOFA, the Oracle Fusion Middleware server was last updated on September 27, 2014. This server was vulnerable to a critical flaw (CVE-2021-35587), which impacts Oracle Access Manager (OpenSSO Agent). This vulnerability was added to the CISA KEV (Known Exploited Vulnerabilities) list in December 2022.

4. Critical Vulnerability

CVE-2021-35587: Vulnerability in Oracle Access Manager (OpenSSO Agent).

A critical vulnerability exists in the Oracle Access Manager component of Oracle Fusion Middleware (OpenSSO Agent), affecting versions: 11.1.2.3.0, 12.2.1.3.0 & 12.2.1.4.0

This easily exploitable vulnerability allows an unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful exploitation can lead to a complete takeover of Oracle Access Manager.



The threat actor claimed to an independent news source that they compromised a vulnerable version of Oracle Cloud servers using a public CVE (flaw), which currently lacks a public proof of concept (PoC) or exploit.

As seen in the screenshot above, the login endpoint was last updated in 2014 according to FOFA results. In response, we began investigating older CVEs with high impact on the technology stack and discovered CVE-2021-35587, which affects Oracle Fusion Middleware. This vulnerability has only one known public exploit.

Due to poor patch management practices and/or insecure coding, the vulnerability in Oracle Fusion Middleware was successfully exploited by the attacker. This flaw allows an unauthenticated attacker with network access to compromise Oracle Access Manager. Successful exploitation can lead to a complete takeover of Oracle Access Manager (OAM), which is consistent with the data leaked on Breachforums.

5. Impact of the Breach

- **Mass Data Exposure:** The compromise of 6 million records, including sensitive authentication-related data, heightens the risk of unauthorized access and corporate espionage.
- **Credential Compromise:** The exposure of encrypted SSO and LDAP passwords - if decrypted - could lead to further breaches across Oracle Cloud environments.
- **Extortion & Ransom Demands:** The threat actor is coercing affected companies to pay for the removal of their stolen data, leading to financial and reputational risks.
- **Zero-Day Exploitation:** The suspected use of a zero-day vulnerability underscores significant concerns about Oracle Cloud security and the potential for future attacks.
- **Supply Chain Risks:** The exposure of JKS files and key files could enable attackers to pivot and compromise multiple interconnected enterprise systems, escalating the overall risk.

6. Mitigation Actions

- **Immediate Security Measures**
 - Reset Passwords: Reset all LDAP user account passwords, with a focus on privileged accounts (e.g., Tenant Admins). Enforce strong password policies and Multi-Factor Authentication (MFA) to enhance security.
 - Regenerate API Keys: Revoke and regenerate all API keys to prevent unauthorized access. Implement tighter access controls, restrict key usage, and monitor API activity for anomalies.
 - Rotate SSO Certificates: Regenerate and replace all SSO/SAML/OIDC certificates to ensure secure authentication processes. Enforce certificate rotation policies and secure storage practices.
 - Audit and Update ACL: Review and harden Access Control Lists (ACLs) to restrict access to trusted IP ranges only. Implement geo-restrictions, IP allowlisting, and firewall rules to minimize exposure.
 - Update SASL Hashes: Regenerate SASL/MD5 hashes or migrate to a more secure authentication method.
 - Audit and Activity Log Review: How to Detect Suspicious Activity in Oracle Cloud (ref. 6.1)
- **Tenant-Level Credential Rotation**
 - Contact Oracle Support immediately to rotate tenant-specific identifiers (e.g., orclmttenantguid, orclmttenantuname) and discuss additional remediation steps.
- **Regenerate Certificates and Secrets**
 - Regenerate and replace any SSO/SAML/OIDC secrets or certificates associated with the compromised LDAP configuration to mitigate further risks.
- **Audit and Monitoring**
 - Review LDAP logs for any suspicious authentication attempts.
 - Investigate recent account activities to identify potential unauthorized access.
 - Implement continuous monitoring to detect unauthorized access and anomalous behavior in real time.
- **Enhanced Security Protocols**
 - Immediate Credential Rotation: Rotate all SSO, LDAP, and associated credentials, enforcing strong password policies and MFA.
 - Incident Response & Forensics: Conduct a comprehensive investigation to identify the full extent of the breach and mitigate further risks.
 - Threat Intelligence Monitoring: Continuously monitor the dark web and threat actor forums for discussions related to the leaked data and potential exploits.
 - Engage with Oracle Security: Report the incident to Oracle to verify if this was part of a supply chain attack and request patches or mitigations.
 - Strengthen Access Controls: Implement strict access policies, adopt the principle of least privilege, and enhance logging mechanisms to detect and prevent future breaches.

6.1. Audit and Activity Log Review

As part of our security recommendations, we strongly advise organizations to proactively monitor their audit logs and system activity to detect unauthorized access or suspicious behavior. Below are the key steps to verify activity, check for potential intrusions, and set up monitoring for future threats.

- <https://github.com/oci-landing-zones/oci-cis-landingzone-quickstart/blob/main/compliance-script.md>
- <https://docs.oracle.com/en/learn/generating-iam-reports-from-oci-audit/index.html#objectives>

6.1.1. Monitor Audit Logs for Suspicious Activity

Oracle Audit Logs track all API calls, including logins, resource modifications, and key changes.

Check for unauthorized access.

Steps to review audit logs in OCI:

1. Go to: **OCI Console** → **Governance & Administration** → **Audit**
2. Select: Your **tenancy or a specific compartment**
3. Filter events by:
 - a. **Event Type**: CreateSession (logins), UpdateUser, DeleteUser, ListKeys, Authenticate
 - b. **Source IP Address**: Look for unknown or foreign locations
 - c. **User/Principal**: Identify unexpected users making API requests
4. Click "Search" and review the logs for anomalies

To retrieve recent authentication events via CLI, run:

```
oci audit event list --start-time "2024-03-25T00:00:00Z" --end-time "2024-03-25T23:59:59Z" --compartment-id <COMPARTMENT_OCID>
```

Look for unexpected IP addresses, unusual login patterns, or privilege escalations

Check Compute Instances for Active Sessions

If an attacker has gained access to a Compute Instance, they might still have an active session. View active SSH sessions:

Run these commands to check logged-in users:

- **who**
- **w**
- **last -a | head -10**

Look for unexpected logins.

Check SSH Logs to see all successful SSH logins:

- **sudo cat /var/log/auth.log | grep "Accepted"**

Look for logins from unknown IPs.

6.1.2. Set Up Continuous Monitoring & Alerts

To track inbound/outbound traffic to your OCI instances:

1. Enable VCN Flow Logs
 - a. Go to **Networking** → **Virtual Cloud Networks (VCN)**
 - b. Select your **VCN** → Click **Flow Logs** → **Create Flow Log**
2. Choose:
 - a. **Subnet**: Public-facing or critical subnets
 - b. **Log Destination**: Store logs in an Object Storage Bucket
3. Analyse logs using OCI Logging Analytics or SIEM tools

To receive real-time notifications for unauthorized access:

1. Go to **Monitoring** → **Alarms** → **Create Alarm**
2. Select **Audit Log Source** and filter on **CreateSession**
3. Configure **notifications** via OCI Notifications Service (Email/SMS)
4. Set a threshold:
 - a. Example: "Alert if more than 1 login from an unknown IP within 5 minutes"

Run this command to trigger alerts for unauthorized logins:

```
oci monitoring alarm create --query "CreateSession AND sourceIp != <your known IP>"
```

Regularly reviewing logs and setting up proactive monitoring can help detect unauthorized access early and prevent further exploitation. We strongly recommend that organizations take immediate action to audit access, revoke unused credentials, and monitor cloud activity continuously.

7. Articles

- <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://www.cloudsek.com/blog/part-2-validating-the-breach-oracle-cloud-denied-cloudseks-follow-up-analysis>
- <https://www.bleepingcomputer.com/news/security/oracle-denies-data-breach-after-hacker-claims-theft-of-6-million-data-records/>
- <https://socradar.io/oracle-cloud-security-incident-by-rose87168/>
- <https://www.esecurityplanet.com/trends/oracle-cloud-breach-6m-records-140k-tenants-risk/>
- <https://www.darkreading.com/cyberattacks-data-breaches/oracle-denies-claim-oracle-cloud-breach-6m-records>
- https://www.linkedin.com/posts/alon-gal-utb_big-i-just-received-10000-records-from-activity-7310017463516127232-XWbI/

8. Data

The sample data included three .txt files, identified as:

- "Company.List.txt": A list of over 140,000 domains belonging to organizations that are purportedly impacted by the breach.
- "Sample_LDAP.txt": Contains LDAP-formatted user information, including user identity, contact details, hashed authentication credentials, group memberships, and Oracle Cloud tenant context. While not necessarily indicative of the entire dataset, Flashpoint analysts have noted that the password expiration dates in this sample are from 2018, suggesting that the data may be old.
- "Sample_Database.txt": 100 rows from a Users table of a database, likely related to the LDAP data. The dates in this sample are from 2022 and 2023.