CloudSEK
REPORTS

21 MAR 2025

Event Report

[GTI] The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants

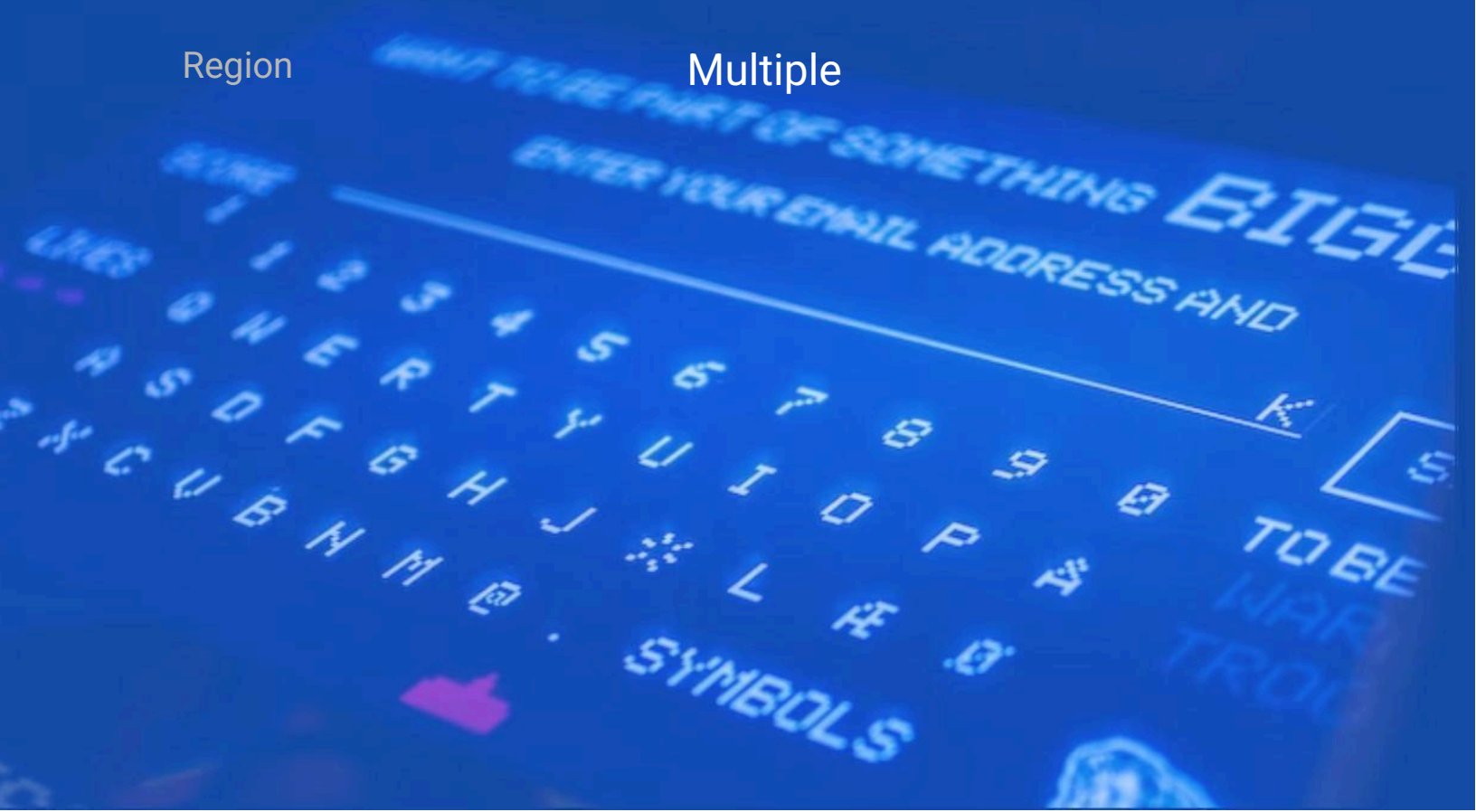
---

Category

Adversary Intelligence

Region

Multiple



TLP#: GREEN

Category:	Industry:	Motivation:	Region:	Source*:
Adversary Intelligence	Multiple	Financial	Multiple	A2

Executive Summary

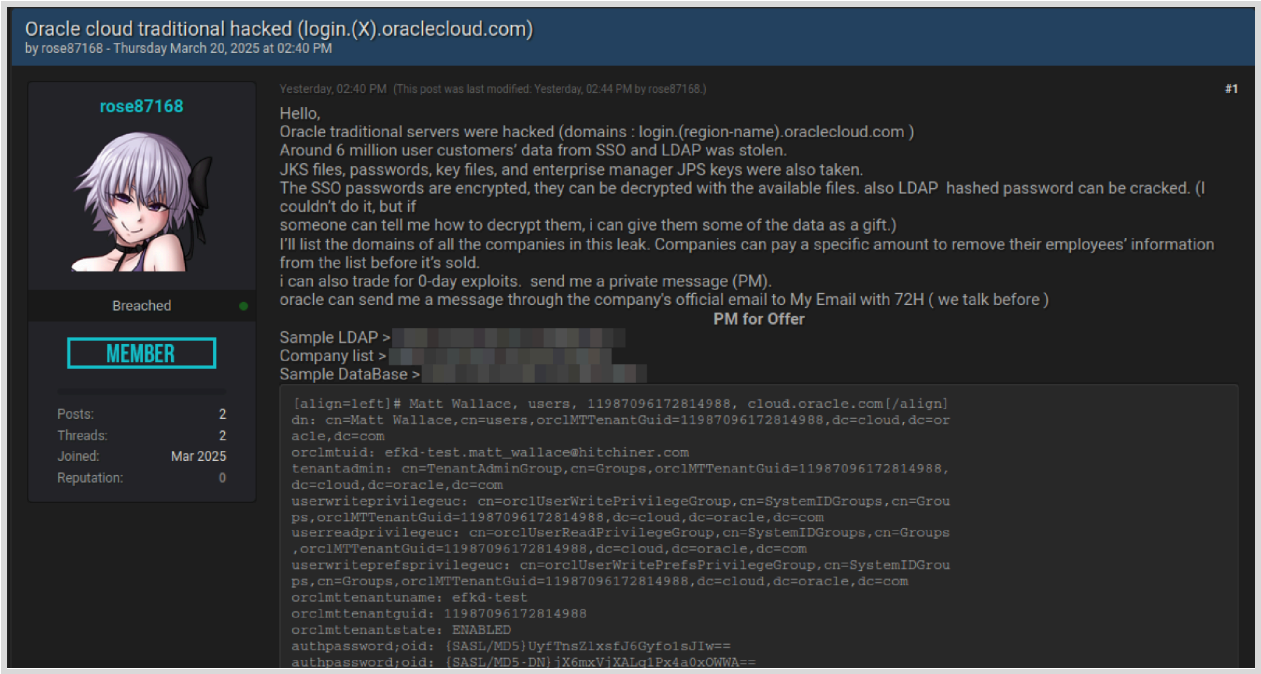
On 21 March 2025, CloudSEK's XVigil discovered a threat actor, "rose87168," selling 6M records exfiltrated from SSO and LDAP of Oracle Cloud. The data includes JKS files, encrypted SSO passwords, key files, and enterprise manager JPS keys.

The attacker, active since January 2025, is incentivizing decryption assistance and demanding payment for data removal from over 140K affected tenants. Our engagement with the threat actor suggests a possible undisclosed vulnerability on login.(region-name).oraclecloud.com, leading to unauthorized access. While the threat actor has no prior history, their methods indicate high sophistication, CloudSEK assesses this threat with medium confidence and rates it as High in severity.

Analysis and Attribution

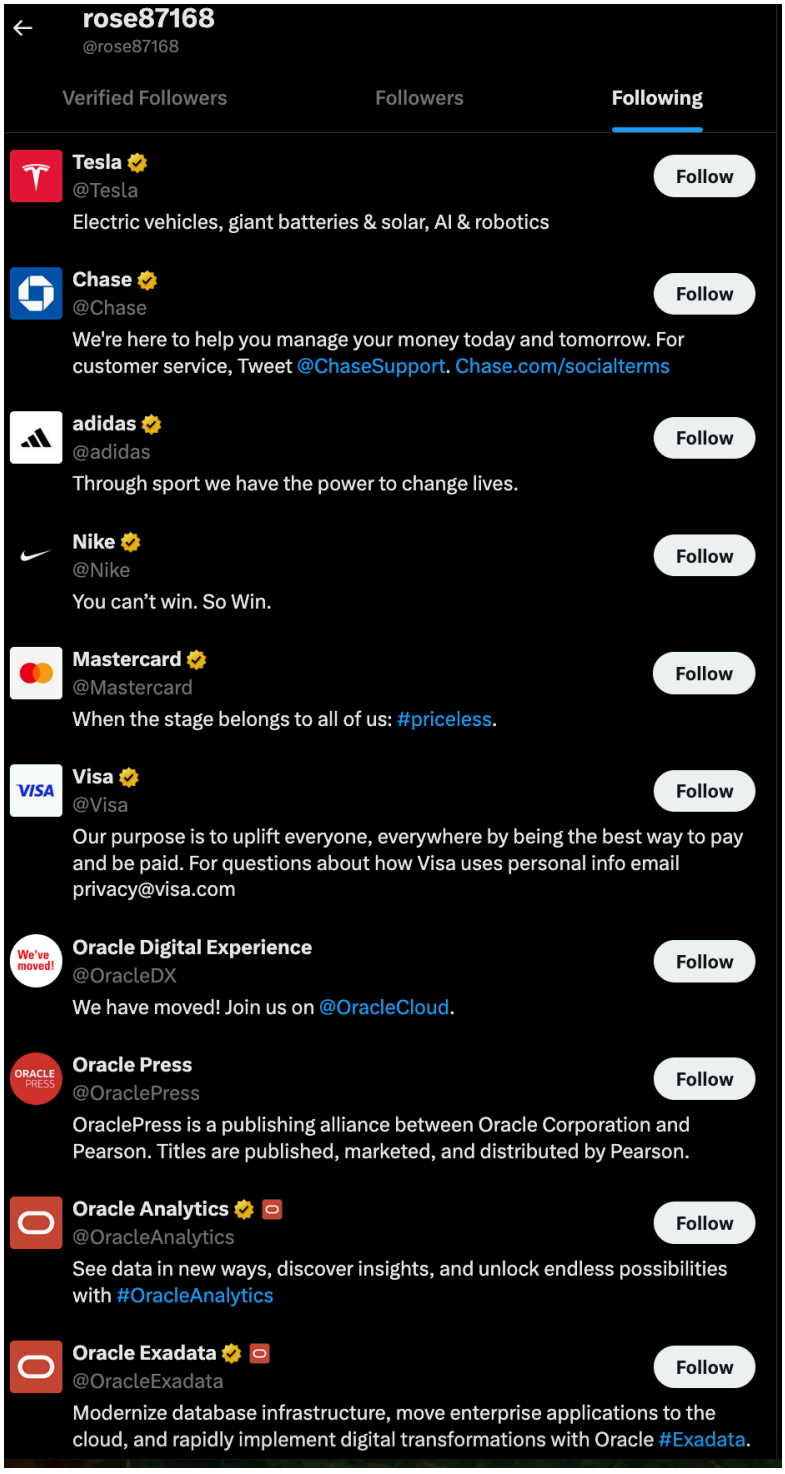
Information from the Post

- CloudSEK's XVigil discovered threat actor "rose87168" selling 6 million records extracted from Oracle Cloud's SSO and LDAP on March 21, 2025. The threat actor claims to have gained access by hacking the login endpoint: *login.(region-name).oraclecloud.com*.



Threat actor listing 6M records exfiltrated from Oracle Cloud

- The database includes:
    - ~6 million lines of data dumped from Oracle Cloud's SSO and LDAP that include
        - JKS files,
        - encrypted SSO passwords,
        - key files,
        - enterprise manager JPS keys.
- Additionally, the threat actor offered an incentive to anyone that helped them decrypt the SSO passwords, and/or crack the LDAP passwords.
- The list of affected tenants is over 140k, and the threat actor is urging companies to contact them and pay a certain "fee" to get their data removed.
- The threat actor also created an X page and started following Oracle related pages.



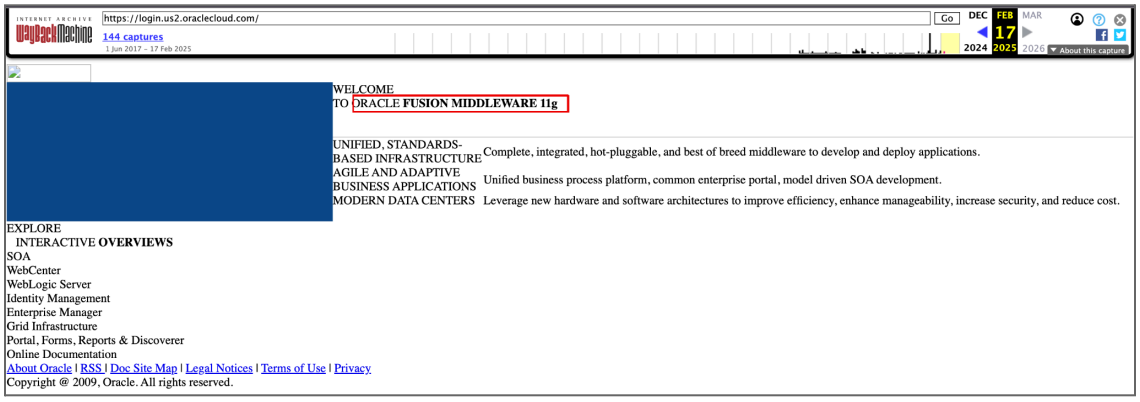
Screenshot of the threat actor's X account following list

Analysis :

The threat actor claimed to have compromised the subdomain login.us2.oraclecloud.com, which has been claimed to have been taken down since the hack.

Screenshot of the the text file uploaded by the threat actor on the endpoint login.us2.oraclecloud.com

The subdomain was captured on the wayback machine on 17 Feb 2025, which suggests that it was hosting Oracle fusion middleware 11G .



Screenshot of the login.us2.oraclecloud.com on wayback machine

The oracle fusion middleware server , which according to the fofa were last updated around Sat, 27 Sep 2014 . The Oracle fusion middleware had a critical vulnerability CVE-2021-35587 which affects Oracle Access Manager (OpenSSO Agent) . Which was added to CISA KEV(Known Exploited Vulnerabilities) on 2022 December.

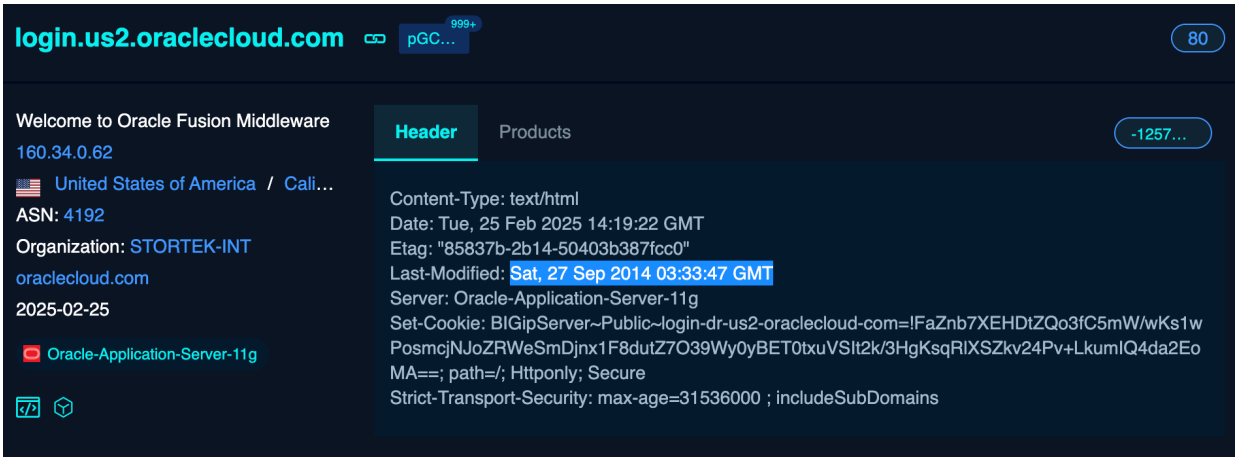
CVE-2021-35587: Vulnerability in Oracle Access Manager (OpenSSO Agent)

A vulnerability exists in the Oracle Access Manager component of Oracle Fusion Middleware (OpenSSO Agent). The affected versions are:

- 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.



Screenshot from fofa showcasing the endpoint login.us2.oraclecloud.com

Threat actor claimed to one of the independent news sources that they have compromised a vulnerable version of the Oracle Cloud servers with a public CVE (flaw) that does not currently have a public PoC or exploit.

As we can see in the aforementioned screenshot, the login endpoint was last updated in 2014 as per FOFA results. Consequently, we started looking for any older CVEs with high impact affecting the technology stack. In that process, we found an older CVE affecting Oracle Fusion Middleware (CVE-2021-35587) that only has a single known public exploit.

Due to lack of patch management practices and/or insecure coding, the vulnerability in Oracle Fusion Middleware was exploited by the threat actor. This easily exploitable vulnerability allows an unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in takeover of Oracle Access Manager(OAM). This aligns with the samples that were leaked on Breachforums too.

Threat Actor Activity and Rating

Threat Actor Profiling	
Active since	Jan 2025
Reputation	0
Current Status	ACTIVE
History	A new user on the forum with no history of previous attacks. However, the samples and supporting information shared by the threat actor points towards a high sophistication.
Rating	High

Impact

- **Mass Data Exposure:** Compromise of 6M records, including sensitive authentication-related data, increases risks of unauthorized access and corporate espionage.
- **Credential Compromise:** Encrypted SSO and LDAP passwords, if cracked, could enable further breaches across Oracle Cloud environments.
- **Extortion & Ransom Demands:** Threat actor is coercing affected companies to pay for data removal, increasing financial and reputational risks.
- **Zero-Day Exploitation:** The suspected use of a zero-day vulnerability raises concerns about Oracle Cloud security and potential future attacks.
- **Supply Chain Risks:** Exposure of JKS and key files may enable attackers to pivot and compromise multiple interconnected enterprise systems.

Mitigation

- **Immediate Security Measures**
    - Reset Passwords: Immediately reset passwords for all compromised LDAP user accounts, focusing particularly on privileged accounts (e.g., Tenant Admins). Enforce strong password policies and MFA.
    - Update SASL Hashes: Regenerate SASL/MD5 hashes or migrate to a more secure authentication method.
- **Tenant-Level Credential Rotation**

  - Contact Oracle Support immediately to rotate tenant-specific identifiers (e.g., orclmttenantguid, orclmttenantuname) and discuss necessary remediation steps.
- **Regenerate Certificates and Secrets**
  - Regenerate and replace any SSO/SAML/OIDC secrets or certificates associated with the compromised LDAP configuration.
- **Audit and Monitoring**
  - Review LDAP logs for suspicious authentication attempts.
  - Investigate recent account activities to detect potential unauthorized access.
  - Implement continuous monitoring to track unauthorized access and anomalous behavior.
- **Enhanced Security Protocols**
  - Immediate Credential Rotation: Rotate all SSO, LDAP, and associated credentials, ensuring strong password policies and enforcing Multi-Factor Authentication (MFA).
  - Incident Response & Forensics: Conduct a comprehensive investigation to identify potential unauthorized access and mitigate further risks.
  - Threat Intelligence Monitoring: Continuously monitor dark web and threat actor forums for discussions related to the leaked data.
  - Engage with Oracle Security: Report the incident to Oracle for verification of a potential supply chain attack and seek patches or mitigations.
  - Strengthen Access Controls: Implement strict access policies, adopt the principle of least privilege, and enhance logging mechanisms to detect anomalies and prevent future breaches.

References

- *Intelligence source and information reliability - Wikipedia
- #Traffic Light Protocol - Wikipedia

CloudSEK

We Predict Cyber Threats

Monitor. Analyse. Predict.

Secure your Tomorrow,Today!

Request for a Free Demo of our platform:

SCAN ME

OR

Mail us at **info@cloudsek.com**
or visit **https://cloudsek.com**

Gain access to a free trial and Detailed POC on CloudSEK Platform

Registered Office:

CloudSEK Research Pte Ltd.
51 Chin Swee Rd. #07-12 Manhattan House,
Singapore 169876

Regional Office: United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901
United States

Regional Office: India

CloudSEK Information Security Pvt Ltd
16/1, WINGS, Cambridge Rd, Halasuru,
Cambridge Layout, Jogupalya,
Bengaluru, Karnataka, India - 560008

Regional Office: United Kingdom

CloudSEK, 4th floor, Rex House,
4, 12 Regent Street, London,
SW1Y 4PE - United Kingdom