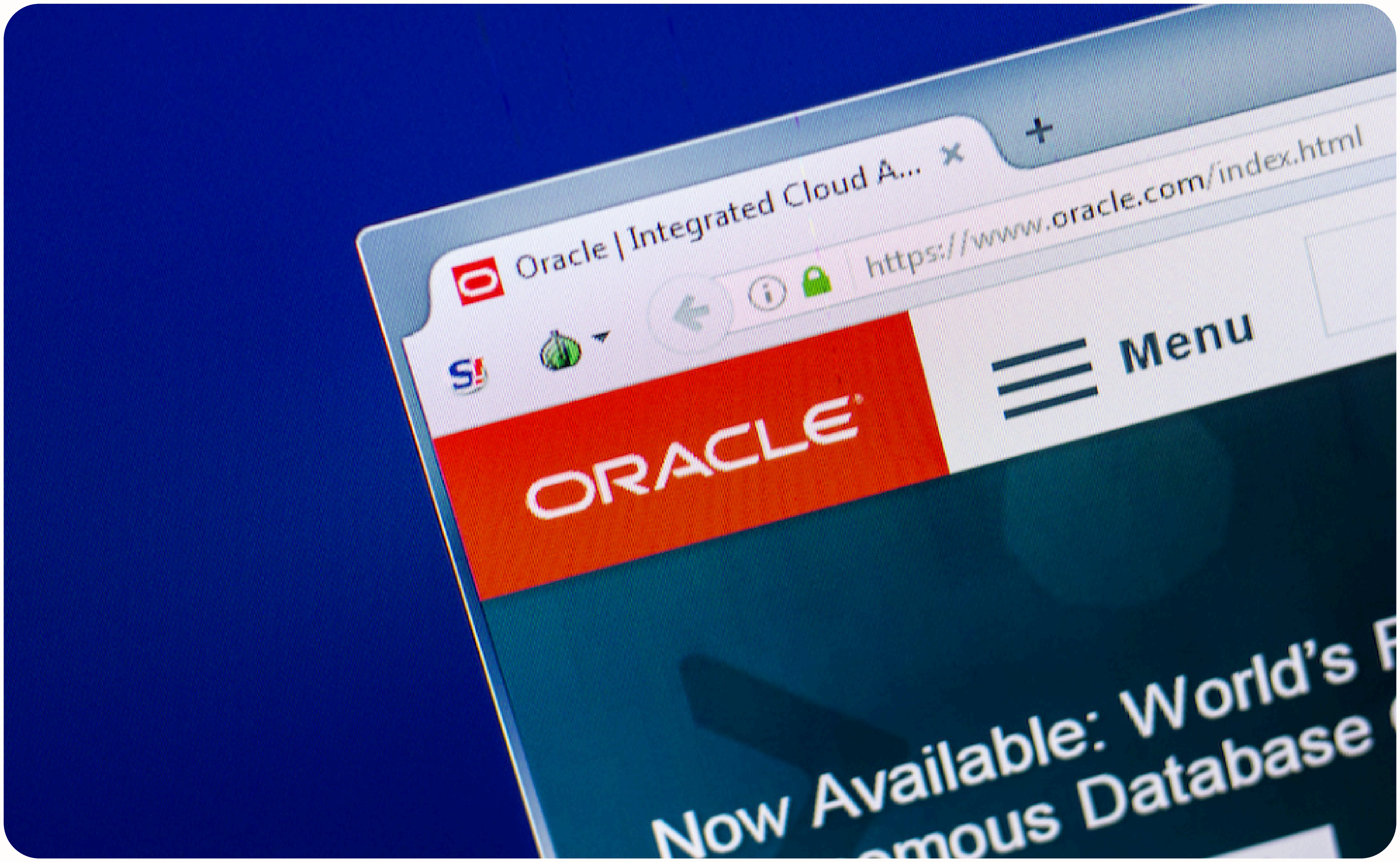

Oracle | Integrated Cloud A...
https://www.oracle.com/index.html
ORACLE
Menu
Now Available: World's F
omous Database

Massive Oracle Cloud Breach

6 Million Records Exfiltrated in Sophisticated Cyberattack

www.clovinsec.com

1.INTRODUCTION

- Security vendor CloudSEK recently exposed a massive breach in Oracle Cloud, **compromising 6 million records.**
- The breach, affecting over **140,000 tenants, involved sensitive data like JKS files** and encrypted SSO passwords.
- A threat actor, **"rose87168,"** exploited a suspected undisclosed vulnerability, demanding ransom for the stolen data.
- **Despite Oracle's denial,** evidence suggests a serious security lapse with far-reaching implications.
- This post breaks down the technical details, execution, and expert insights into this critical incident.

2. TECHNICAL BREAKDOWN

- The attack demonstrates the need for robust vulnerability management and patching strategies.
- The breach targeted **Oracle Cloud's SSO and LDAP systems, exfiltrating 6M records including JKS files (Java KeyStore) for cryptographic keys.**
- **Encrypted SSO passwords and Enterprise Manager JPS keys were stolen,** critical for authentication and access control.
- CloudSEK suspects a **zero-day vulnerability in Oracle WebLogic Server,** possibly **CVE-2021-35587 (CVSS 9.8)**, **unpatched since 2014.**
- The login endpoint **"login.(region-name).oraclecloud.com"** was the entry point, exposing tenant data across regions.
- Data was dumped via sophisticated exploitation, highlighting weaknesses in Oracle's cloud infrastructure security.

www.clovinsec.com

3. ATTACK EXECUTION DETAILS

- The attacker, **"rose87168,"** began operations in January 2025, compromising **"login.us2.oraclecloud.com" by mid-February.**
- Using an unpatched flaw, they **extracted 6M records and uploaded a text file to the server as proof (archived on Wayback Machine).**
- Data was advertised on **BreachForums on March 21, 2025,** with samples showing real tenant domains like sbgtv.com.
- The **actor offered decryption assistance** incentives and demanded ransoms, escalating pressure on affected organizations.
- **Oracle took the subdomain offline post-breach**, but not before significant data exposure occurred.

4. UNDERLYING MOTIVATIONS

- Financial gain drives **"rose87168,"** who **demanded 100,000 XMR (~$200M)** from Oracle for vulnerability details.
- **Selling 6M records** on dark web forums like BreachForums aims to maximize profit from stolen credentials.
- **Extortion of 140,000+ tenants** reflects a strategy to exploit corporate fear of data leaks and reputational damage.
- The actor’s sophistication suggests a targeted hit on a **high-value cloud provider** to establish credibility.
- Lack of prior history indicates a new player testing the waters with a high-stakes supply chain attack.

5. ADDITIONAL NEWS & UPDATES

- Oracle denied the breach on **March 22, 2025,** claiming no **customer data was lost,** contradicting CloudSEK's findings.
- **CloudSEK's follow-up on March 25** validated the breach with a **10,000-line sample,** confirmed by **BleepingComputer.**
- Posts on X from **@NSIguy and @TweekFawkes (March 26-27)** highlight ongoing debates over Oracle's security.
- **CVE-2021-35587, tied to Oracle Fusion Middleware, remains a focal point for vulnerability discussions**.
- The incident underscores rising **supply chain attack trends, per Arctic Wolf's 2025** Threat Report.

6. EXPERTS RECOMMENDATIONS

- **CloudSEK's Rahul Sasi** emphasizes transparency, urging i**mmediate credential rotation and MFA enforcement.**
- **Chad Cragle (Deepwatch CISO)** questions Oracle's denial, citing the uploaded file as evidence of access.
- **Heath Renfrow (Fenix24**) recommends auditing SSO configs and monitoring for compromise indicators.
- **Reset all LDAP/SSO passwords,** regenerate JKS files, and conduct forensic probes, per CloudSEK's advisory.
- Experts warn of supply chain risks; organizations must enhance patch management and dark web monitoring.

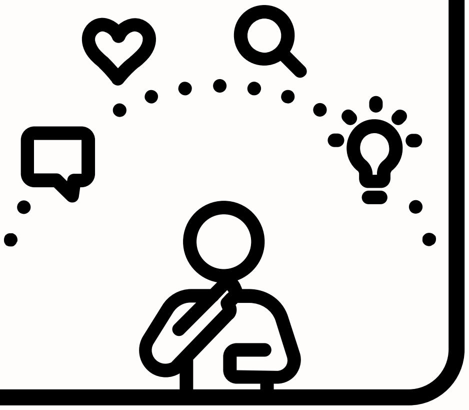
REFERENCE

- CloudSEK Report
- BleepingComputer: Oracle Denies Breach
- Dark Reading: Oracle Cloud Breach
- Hackread: CloudSEK Disputes Oracle
- X Post by @NSIguy
- Cybersecurity Dive: Researchers Back Claim
- eSecurity Planet: Oracle Cloud Breach

CLOVIN SECURITY:

YOUR TRUSTED CYBER DEFENSE PARTNER

- Specialized in Vulnerability Assessment and Penetration Testing (VAPT) to fortify your systems.
- AI-powered Pentesting for smarter, faster security testing.
- Real-time threat detection and tailored strategies to outpace cyber threats.
- Expert cloud, network, and compliance security solutions for businesses of all sizes.
- 24/7 cybersecurity support to safeguard your digital ecosystem with Clovin Security.



CLOVIN
SECURITY

www.clovinsec.com

Stay Updated With Us..!

For More Information

www.clovinsec.com

Clovin Security (1.5k+)

@clovin_sec (460+)

info@clovinsec.com

Like Comment Save Share