



| Flash |

Situation Report: Alleged Oracle Breach

F-2025-03-26a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Data Breach, Threat Actor

March 26, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 26, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Situation Report: Alleged Oracle Breach

| Key Findings

- As of this writing, stolen data allegedly associated with U.S.-based technology firm Oracle has not been shared in its entirety or sold to any known actor or entity, and although some alleged victims have confirmed the data is legitimate, investigations are ongoing.
- On March 20, 2025, actor “rose87168” posted in the predominantly Russian-speaking forum BreachForums, claiming to have stolen data associated with six million users of Oracle Cloud services.
- Rose87168 did not disclose the asking price of the full dataset, instead urging prospective buyers to make contact. The actor further specified that organizations can pay “a specific amount” to have their data deleted before it is sold.
- The data’s utility in conducting subsequent exploitative activity—such as the further compromise of downstream and adjacent Oracle services or accessing sensitive and proprietary information held within workspaces—is heavily dependent on individual use and security configuration.

- There is a very likely chance that the threat posed to alleged victims will be lessened by the time any purchase takes place, as organizations enact precautionary security procedures to mitigate the impact of subsequent exploitation.

| Details

On March 20, 2025, actor rose87168 posted in the predominantly Russian-speaking forum BreachForums, claiming to have stolen data associated with six million users of Oracle Cloud services. These claims were subsequently denied by Oracle.

- According to the advertisement, the exfiltrated data includes JKS files (commonly used for storing private keys and certificates), encrypted SSO passwords, and enterprise manager JPS keys.
- Data samples accompanied the advertisement, including an alleged victim list, a sample database, and a sample of stolen LDAP data.
- On March 25, rose87168 posted in the thread claiming that an additional data offering comprising 10,000 samples is available to threat researchers that provide a corporate email address. This is very likely reflective of rose87168 attempting to verify the legitimacy of their claim and to encourage alleged victim organizations to make contact.

Oracle cloud traditional hacked (login.(X).oraclecloud.com)
by rose87168 - Thursday March 20, 2025 at 02:40 PM

👑 rose87168



GOD User

GOD

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

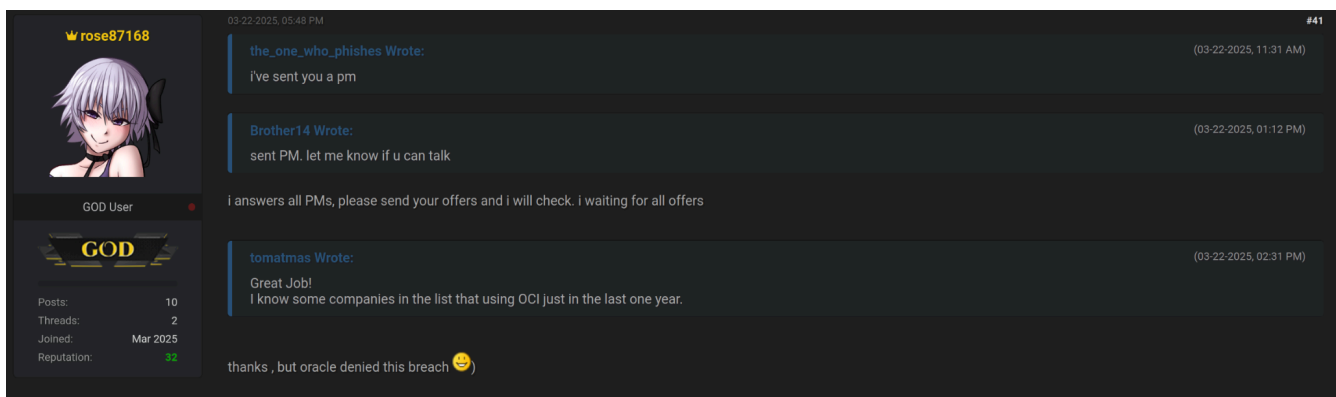
Sample LDAP > [REDACTED]
Company list > [REDACTED]
Sample DataBase > [REDACTED]

rose87168 advertises alleged breach in BreachForums

Source: ZeroFox Intelligence

Rose87168 did not disclose the asking price of the full dataset, instead urging prospective buyers to make contact. The actor further specified that organizations can pay "a specific amount" to have their data deleted before it is sold. No negotiations have yet been observed, though any such communications would very likely take place in private channels.

- Reporting suggests that rose87168 demanded approximately USD 22 million from Oracle to be paid via approximately 100,000 XMR (Monero), which was refused.
- Rose87168 has not publicly advertised a sale price for the alleged data to other potential buyers, but the exorbitant price of 100,000 XMR is very unlikely to be met.
- If the sample information provided by the actor accurately reflects the data for sale, it will very likely be perceived as potentially lucrative by financially motivated threat actors.



rose87168 alludes to alleged Oracle denial

Source: ZeroFox Intelligence

Rose87168's post spurred significant conversation surrounding the data's legitimacy, with some actors suggesting that the data had been stolen from a testing or "non-production line" environment.

- One such actor was promptly banned, though ZeroFox notes that this was very likely in response to multiple spam-like posts in the thread.

At least some of the data samples observed by ZeroFox suggest association with a "canary" environment; however, it remains unclear how this impacts the sensitivity of the

alleged data. Upon engagement by ZeroFox researchers, rose87168 denied that any of the allegedly stolen data originated from a testing or non-product environment.

- Another actor asserted that, by listing all the allegedly compromised organizations, rose87168 had afforded them the opportunity to secure their attack surfaces—thereby lessening the likelihood of both victim payment for data removal and subsequent compromise at the hands of prospective buyers.

As of the writing of this report, the threat of subsequent exploitation posed to the alleged victim organizations listed by rose87168 remains unclear. If the compromise is legitimate and as advertised, this would almost certainly constitute a significant proportion of corporate personally identifiable information (PII) being made available for purchase.

Should an actor obtain the advertised information, they would almost certainly encounter subsequent security challenges. ZeroFox notes an apparent lack of the information and leverage needed to easily conduct exploitative activity, such as decrypted passwords and the necessary tokens and certificates. These requirements will vary significantly between organizational Oracle logins, applications, and workspaces.

- The data's utility in conducting subsequent exploitative activity—such as the further compromise of downstream and adjacent Oracle services or the accessing of sensitive and proprietary information held within workspaces—is heavily dependent on individual use and security configuration.

There is a very likely chance that the threat posed to alleged victim organizations upon initial compromise will be lessened by the time any purchase takes place. Their being listed by rose87168 will almost certainly lead to at least some of the alleged victim organizations enacting precautionary security procedures to mitigate subsequent exploitation, such as resetting passwords associated with LDAP user accounts and ensuring that appropriate multi-factor authentication (MFA) protocols are in place.

| Recommendations

- Organizations appearing on the alleged victim list should enact preemptive cyber hygiene procedures, such as rotating credentials and refreshing tokens and certificates associated with logins.
- Use open source tools to proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Ensure the security protocols of Oracle accounts, workspaces, and downstream services are appropriately configured and reflect the sensitivity of associated data.
- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%