VISION by protiviti

In Focus

29 April 2025

Oracle Cloud security: Preventing unauthorised access and data theft

By David Taylor
Managing Director

Data compromises have increasingly plagued organisations worldwide, underscoring the urgent need for robust security measures. The latest reported incidents involving Oracle have spotlighted the critical importance of protecting customer data. These breaches resulted in the theft of sensitive information, emphasising the necessity for comprehensive security protocols. To safeguard your Oracle Cloud instance and prevent unauthorised access, it is imperative to understand and implement effective protective steps.

Why it matters

Recently reported breaches highlight the critical need for companies to secure login credentials and sensitive customer data. These incidents involved the theft of active login credentials, posing a significant risk of unauthorised access and potential misuse of information.

Although Oracle has assured its cloud infrastructure remains uncompromised, it is imperative for organisations to take proactive steps to safeguard their data. This vigilance is essential to prevent similar breaches and protect valuable corporate information. For example, the theft of login credentials can lead to unauthorised access to sensitive data, which can have far-reaching consequences, including financial losses, reputational damage and legal liabilities.

Despite assurances from vendors, it is imperative that organisations take necessary steps to better secure their cloud instances and take an active role in protecting data from compromise. For Oracle users and others, many of the following immediate steps will prove instrumental in further protecting data from theft or exposure:

- **Change passwords and enable MFA.**
    - Change all passwords using strong passwords or passphrases.
    - Implement multi-factor authentication (MFA) wherever possible.
    - Update any hardcoded script or service passwords that may have been compromised.
- **Review access logs for anomalous behaviour.**
    - Thoroughly review access logs and single sign-on (SSO) logs for signs of unauthorised access or abuse.
    - If no evidence of unauthorised activity is found, the organisation was likely not impacted.
    - If evidence of abuse is detected, initiate an incident response process to contain and mitigate the breach.
- **Enhanced monitoring for high-risk clients.**
    - Implement additional monitoring for federated identity accounts of sensitive or high-risk clients.
    - Scrutinise anomalous behavior closely for an extended period to ensure no further compromise occurs.
- **Utilise Oracle's vulnerability detection service.**
    - Use Oracle's vulnerability detection service to identify and address any unpatched vulnerabilities in Oracle environments.
- **Dark Web monitoring.**
    - Monitor the darknet for signs of compromised credentials or data being sold.
    - Take immediate action if any compromised data is found.

What they say

Drew Todd, Content and Business Development Strategist at SecureWorld

"In what may become one of the most scrutinised cloud security incidents of 2025, Oracle has come under fire following claims by a threat actor alleging the exfiltration of more than six million records from Oracle Cloud Infrastructure (OCI), potentially impacting more than 140,000 tenants."

What we say

The recently claimed Oracle breaches serve as a stark reminder of the critical importance of securing login credentials and sensitive customer data. These purported incidents involved the theft of active login credentials, which pose a significant risk of unauthorised access and potential misuse of information. Although Oracle assures clients that their cloud infrastructure remains uncompromised, the alleged breaches underscore the necessity for organisations to adopt proactive measures to safeguard their data. In today's digital landscape, the protection of login credentials is paramount. The stolen data from such breaches may include active login credentials, which could be exploited by malicious actors to gain unauthorised access to sensitive information. This potential misuse of data highlights the vulnerabilities that organisations face and the urgent need for robust security protocols.

The bottom line

Organisations must take proactive steps to protect their data. Additionally, regular security audits and investing in advanced threat detection systems are essential to mitigate the risk of breaches. Employee training on best practices for data security is also crucial to ensure that all members of the organisation are equipped to handle potential threats. In addition to the near-term steps listed above, it is important for organisations to take the necessary long-term security measures to protect data from compromise, including:

- **Reset passwords based on identity federation configuration**
    - Reset passwords for all system user accounts if using an external identity provider with MFA enabled and the chooser page disabled.
    - Reset passwords for all local users and system accounts if using an external identity provider with MFA enabled and the chooser page enabled.
    - Reset passwords for all system user accounts, local end users, and external identity providers if using an external identity provider without MFA enabled and the chooser page disabled.
    - Reset passwords for all system user accounts, local end users, and external identity providers if using an external identity provider without MFA enabled and the chooser page enabled.
    - Reset every user's password if using native login in Oracle Cloud.

- **Eliminate basic authentication**
    - Eliminate basic authentication for all integrations to reduce the risk of credential theft.
    - Enable WAF4SaaS to restrict client network access and implement label-based access control (LBAC) or IP allowlisting.
- **Enable audits and monitor suspicious activities**
    - Enable all necessary audits to monitor activities such as role changes, role provisioning, and password resets.
    - Keep a close watch on any suspicious activities and take immediate action if any anomalies are detected.
- **Rotate API and auth token keys**
    - Regularly rotate all API and authentication token keys to minimise the risk of unauthorised access.
    - Rotate all service account passwords and encryption keys to ensure they remain secure.

By following these steps, organisations can significantly enhance the security of their Oracle Cloud instances and protect themselves from potential data breaches. It is crucial to stay vigilant and continuously update security measures to adapt to evolving threats.

Protiviti Senior Manager Uriah Robins contributed to this report.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2025 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a CMMCAB RPO organisation and has been supporting companies with CMMC services for seven years. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business in the future. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

protiviti®