Searchlight Cyber Discloses Critical Pre-Authentication Vulnerability in Oracle Identity Manager

Critical 9.8 CVSS flaw in Oracle Identity Manager allowed pre-authentication remote code execution, discovered and responsibly disclosed by research team

PORTSMOUTH, UNITED KINGDOM, November 20, 2025 /EINPresswire.com/ -- Searchlight Cyber today announced the discovery of a critical zero-day vulnerability in Oracle Identity Manager (OIM), a widely deployed identity and access management product used across global enterprises.

The flaw, now acknowledged by Oracle with a CVSS score of 9.8, enabled pre-authentication remote code execution - one of the most severe forms of compromise against identity infrastructure.

Earlier this year, in January, Oracle Cloud's login service suffered a serious data breach due to vulnerabilities in Oracle Access Manager. By investigating this breach and Oracle's various identity-related products, Searchlight Cyber's Security Research team discovered a pre-authentication RCE vulnerability in Oracle Identity Manager, which was also found to be running on Oracle Cloud's login service.

This new and previously unreported vulnerability can lead to the breach of servers handling user PII and credentials, underscoring the systemic nature of vulnerabilities within Oracle's identity management and access stack. Oracle has formally credited Searchlight researchers for the discovery.

Analysis showed that Oracle Identity Manager was susceptible to an authentication bypass vulnerability, allowing an attacker to access an endpoint that executed arbitrary code. This enabled a pathway to achieve remote code execution without authentication, granting full system compromise on affected installations.

Searchlight disclosed the issue to Oracle under responsible disclosure protocols and provided a

90-day remediation window. During that period, Searchlight customers were protected from potential exploitation long before any public advisory or proof-of-concept existed. A detailed description of how this vulnerability was uncovered can be found on the Searchlight Security Research Center.

“Since Oracle Identity Manager stores user credentials and PII, it is a prime target for attackers,” said Shubham Shah, SVP of Security Research at Searchlight Cyber. “It’s remotely exploitable, requires no authentication, and is extremely simple for an attacker to exploit. Because we discovered the vulnerability rather than analysing it after exploitation, our customers had months of protection before the wider industry became aware of the risk.”

A compromise of Oracle Identity Manager could allow attackers to manipulate authentication flows, escalate privileges, and move laterally across an organisation’s core systems. For enterprises that rely on OIM, the business impact of this class of vulnerability is significant.

Ben Jones, CEO and Co-Founder of Searchlight Cyber, said, “Reactive intelligence will always have a role, but on its own it isn’t enough. Early discovery gives defenders time, and time is one of the most meaningful advantages in cybersecurity. This is what preemptive security looks like in practice - identifying issues before they appear in advisories or begin to circulate in the wild, and giving organisations the opportunity to act ahead of the threat. I’m incredibly proud of the work our research team continues to deliver, and this discovery is a strong example of the value that responsible, preemptive security can provide to organisations.”

Oracle has released patches for this issue as part of its Critical Patch Update. Searchlight Cyber encourages all organisations using Oracle Identity Manager to apply the update as soon as possible. Searchlight’s full technical analysis will be published today, 20 November 2025, following the end of the responsible disclosure period.

About Searchlight Cyber:

Searchlight Cyber was founded in 2017 with a mission to stop threat actors from acting with impunity. Its Preemptive Threat Exposure Management Platform helps organizations to identify and protect themselves from emerging cybercriminal threats with Attack Surface Management and Threat Intelligence tools designed to separate the signal from the noise. It is used by some of the world’s largest enterprises, government and law enforcement agencies, and the Managed Security Service Providers at the forefront of protecting customers from external threats. Find out more at www.slcyber.io or follow Searchlight Cyber on LinkedIn and Twitter.

Charlotte Rhodes
Searchlight Cyber
c.rhodes@slcyber.io
Visit us on social media:

LinkedIn
X
