Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

October 15, 2025

On-Premises Oracle EBS Systems at Risk Due to CL0P Exploit

By Amy S. Mushahwar, Kathleen A. McGee, and Carly E. Nixon

Many Ransom Emails Sent Already, Coordinate With Your Security and IT Teams To Determine Business Risk

A recent campaign by the CL0P ransomware group has targeted on-premises, customer-managed Oracle E-Business Suite (EBS) systems, resulting in the potential for widespread data exfiltration and extortion attempts. The campaign, observed from late July through early October 2025, leveraged several small and medium vulnerabilities in Oracle EBS, prompting urgent advisories and investigative efforts from security vendors and Oracle Corp.

Oracle issued an emergency patch for a newly discovered vulnerability in Oracle EBS, identified as CVE-2025-61884. This vulnerability allows unauthenticated attackers to remotely execute code on affected systems, posing a significant security risk. As discussed in a recent FBI Cyber Division post, "if your EBS environment is reachable on the network, and especially if it's internet facing, it's at risk for full compromise." The vulnerability was discovered after reports emerged of the CL0P ransomware group exploiting it to gain unauthorized access to Oracle EBS environments. Oracle strongly advises all users to apply the emergency patch immediately to mitigate the risk of exploitation, and we recommend further actions to detect whether your EBS environment may have been compromised already.

Given that CL0P has a long history of exploiting clients through table stakes technologies common in many enterprises, we urge you to take this incident seriously and examine on-premises versions of Oracle EBS. Consistent with past attacks, CL0P has been sending extortion emails to multiple organizations, threatening to leak stolen data unless ransoms are paid. Harvard University and others have reported receiving notice from CL0P.

Basic Timeline and Background

- July 2025: Oracle released a Critical Patch Update (CPU) addressing 309 vulnerabilities, including nine specific to Oracle EBS.
- Late July to Early September 2025: CL0P exploited vulnerabilities in unpatched, internet-facing Oracle EBS systems to gain unauthorized access, enumerate data, and exfiltrate sensitive information.
- Late September to Early October 2025: A coordinated extortion campaign emerged, with CL0P sending mass emails to affected organizations, threatening to leak or sell exfiltrated data unless contacted for ransom negotiations.

The extortion emails, sent from hundreds of compromised accounts across legitimate organizations, referenced CL0P's reputation and provided contact details matching those on CL0P's leak site. An example of CL0P's extortion email related to this attack is available at https://www.bleepingcomputer.com/news/security/harvard-investigating-breach-linked-to-oracle-zero-day-exploit/amp/. Incident response teams confirmed that some sender accounts had been used in prior CL0P operations, indicating a deliberate effort to obfuscate the campaign's origins and evade detection. Many of the extortion emails could hit company spam filters, so we recommend reviewing the sample and searching for the unique contact addresses for this event: support@pubstorm.com and support@pubstorm.net. WatchTower Labs has a helpful breakdown of the exploit chain for further technical information.

CL0P's tactics in this campaign are consistent with its previous data-theft extortion operations, including those targeting Accellion FTA, Fortra GoAnywhere, MOVEit Transfer, and Cleo products. The group is known for rapid exploitation of zero-day vulnerabilities, mass victimization, and extortion without immediate encryption. CL0P's communications have continued to employ a "white knight" narrative, framing their actions as a service rather than a crime.

Oracle's Response

On October 2, 2025, Oracle publicly acknowledged the extortion campaign, confirming that the attacks targeted on-premises, customer-managed EBS systems and involved vulnerabilities addressed in the July 2025 CPU. Oracle strongly advised all EBS users to apply the latest patches and review the security of any internet-exposed EBS instances. The company emphasized that the incident did not involve Oracle's cloud or infrastructure.

Recommended Mitigation and Response

Organizations using Oracle EBS are advised to take the following actions, including but not limited to the appropriate patching. Given that the attackers may have exploited the vulnerabilities before a patch was available, we are recommending investigative actions in addition to immediate and thorough patching.

- Apply the patches to Oracle EBS and all related Oracle components (e.g., Database, Fusion Middleware).
- Integrate Oracle EBS login portals with single sign-on (SSO) and multifactor authentication (MFA) solutions.
- Incorporate web application firewall (WAF), firewall, and web access logging into Security Information Management (SIM) or log aggregation systems for long-term data preservation.
- Review email spam filters and mailbox infrastructure for evidence of CL0P extortion emails, as some may have been blocked.
- For organizations that had not implemented the July 2025 patches before July 31, 2025, conduct a comprehensive digital forensics and incident response (DFIR) investigation to identify potential compromise, including evidence of backdoors, webshells, credential manipulation, and data exfiltration tools.
- Validate and verify patching levels across all Oracle EBS-related products.

Forensic and Investigative Workstreams

DFIR teams are focusing on:

- Inventorying Oracle EBS server infrastructure and backups
- Deploying artifact collection and response tools for investigative analysis
- Reviewing application, operating system, web access, and network traffic logs
- Preserving copies of extortion emails and integrating audit logging for SSO/MFA
- Conducting retroactive threat hunts using endpoint detection and response (EDR/MDR) solutions
- Searching for specific IP addresses and suspicious command lines or scripts associated with the campaign

Conclusion

The CL0P extortion campaign against Oracle EBS underscores the critical importance of timely patching, robust authentication controls, and comprehensive forensic readiness for organizations operating on-premises enterprise applications. But given that many have been exploited already, entities are urged to review their exposure, implement recommended mitigations, and engage in thorough investigative efforts to contain and remediate potential compromise.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

CARLY E. NIXON
Associate
T: 212.419.5889
cnixon@lowenstein.com