

Canon Allegedly Breached by Clop Ransomware via Oracle E-Business Suite 0-Day Hack

 cybersecuritynews.com/canon-breached-clop-ransomware-oracle-ebs-hack

Guru Baran

November 25, 2025



[Home Cyber Attack News](#) Canon Allegedly Breached by Clop Ransomware via Oracle E-Business Suite 0-Day Hack



Canon has officially confirmed that it was targeted during the widespread hacking campaign exploiting a critical zero-day vulnerability in [Oracle E-Business Suite \(EBS\)](#).

The attack, orchestrated by the notorious Clop ransomware gang, has impacted dozens of major organizations worldwide. The group listed Canon on its dark web leak site, publishing the company's domain alongside other alleged victims.

While the listing on the leak site raised concerns about a massive data breach, Canon clarified that the impact was contained. The camera and imaging giant stated that the compromise affected only a specific environment within one of its subsidiaries.

According to the company, the attackers did not encrypt the broader network or disrupt global operations, which distinguishes this incident from the devastating Maze ransomware attack Canon suffered in 2020.

Canon's security team detected the intrusion and immediately isolated the affected systems. In a statement shared with SecurityWeek, the company emphasized that the breach did not spread beyond a web server operated by a Canon U.S.A., Inc. subsidiary.

The rapid containment likely prevented the theft of sensitive customer data or intellectual property, which the Clop group often seeks for extortion.

"We have confirmed that the incident only affected the web server, and we have already taken security measures and resumed service," Canon said. "In addition, we are continuing to investigate further to ensure that there is no other impact".

The Oracle EBS Zero-Day Exploit

The vulnerability used in this campaign is tracked as [CVE-2025-61882](#), a critical security flaw in Oracle E-Business Suite. This zero-day allowed unauthenticated attackers to execute arbitrary code remotely on vulnerable servers.

Security researchers discovered that Clop affiliates, tracked as Graceful Spider, began exploiting this flaw as early as August 2025 to plant web shells and exfiltrate data before Oracle could issue a patch in October.

Detail	Description
CVE ID	CVE-2025-61882
CVSS Score	9.8 (Critical)
Affected Product	Oracle E-Business Suite (EBS)
Affected Versions	12.2.3 through 12.2.14
Vulnerability Type	Unauthenticated Remote Code Execution (RCE)
Exploit Vector	Network (No user interaction required)

This incident is part of a larger “move-it-style” extortion wave where Clop leveraged the zero-day to breach nearly 30 organizations. Instead of deploying encryption malware immediately, the group focused on data theft and subsequently sent extortion emails to executives starting in late [September 2025](#).

These emails threatened to leak stolen documents unless a ransom was paid. The group’s leak site currently lists domains, including Canon, suggesting these entities were successfully compromised during the automated exploitation phase.

Indicators of Compromise (IoCs)

Indicator Type	Value	Description
IPv4 Address	200.107.207.26	Malicious command and control (C2) IP
IPv4 Address	185.181.60.11	Observed exploitation source IP
SHA256 Hash	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d	Malicious zip archive containing exploit tools
SHA256 Hash	6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b	Python script used for server-side exploitation
File Name	FileUtils.java	Malicious web shell downloader

Security teams are advised to scan their Oracle EBS environments for these indicators and apply the official patches immediately to prevent further unauthorized access.

Top 10

[11 Best Enterprise Remote Access Software – 2025](#)

[Top 10 Best Exposure Management Tools In 2026](#)

[15 Best Remote Monitoring Tools – 2025](#)

[Top 10 Best Supply Chain Intelligence Security Companies in 2025](#)

[Top 10 Best Fraud Prevention Companies in 2025](#)