

Exploitation of Oracle E-Business Suite Vulnerability Starts After PoC Publication

Exploitation attempts targeting a critical-severity Oracle E-Business Suite vulnerability have been observed shortly after proof-of-concept (PoC) code was published.

One of the major Oracle product lines, the E-Business Suite is a set of enterprise applications that help organizations automate processes such as supply chain management (SCM), enterprise resource planning (ERP), and customer relationship management (CRM).

Tracked as **CVE-2022-21587** (CVSS score of 9.8), the exploited flaw was identified in the Web Applications Desktop Integrator of Oracle's enterprise product and was addressed as part of Oracle's October 2022 Critical Patch Update.

According to a NIST advisory, unauthenticated attackers with network access via HTTP can easily exploit the security defect to compromise the Web Applications Desktop Integrator and take it over.

This week, CISA added CVE-2022-21587 to its Known Exploited Vulnerabilities (KEV) catalog, urging Oracle customers to apply the available patches as soon as possible.

The first exploitation attempts, however, were observed on January 21, Shadowserver warned last week.

"Since Jan 21st we are seeing exploitation attempts in our honeypot sensors for Oracle E-Business Suite CVE-2022-21587 (CVSS 9.8 RCE) shortly after a PoC was published,"

Shadowserver said.

The PoC came from Vietnam-based cybersecurity firm Viettel Cyber Security, which on January 16 published a detailed analysis of the vulnerability and potential exploitation venues.

According to Shadowserver data, the number of observed exploitation attempts is currently low. However, threat actors are known to target unpatched Oracle products, and the number of attacks may increase shortly.

This week, CISA also warned of observed exploitation of CVE-2023-22952, a high-severity remote code execution flaw in SugarCRM.

Impacting the EmailTemplates, the vulnerability is described as a missing input validation defect that allows an attacker to inject custom PHP code using crafted requests. Patches for this vulnerability were released on January 11, 2023.

In January, shortly after exploitation began, Censys reported seeing hundreds of SugarCRM servers being hacked using CVE-2023-22952.

Related: Exploited Control Web Panel Flaw Added to CISA 'Must-Patch' List

Related: CISA Says Two Old JasperReports Vulnerabilities Exploited in Attacks

Related: CISA Warns Veeam Backup & Replication Vulnerabilities Exploited in Attacks

<https://www.securityweek.com/exploitation-of-oracle-e-business-suite-vulnerability-starts-after-poc-publication/>