

# CVE-2025-61884

## Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability

CISA KEV since Oct 20, 2025

Actively exploited

Ransomware use known

Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: Runtime UI). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

|                                                            |                                                      |                                                                   |                                                                                            |
|------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>91</b>/100</p> <p>Immediate priority</p> | <p>CVSS V3.1</p> <p><b>7.5</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.959</b></p> <p>99.88th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Nov 10, 2025</b></p> <p>KEV since 2025 · listed over a year</p> |
|------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                             |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|---------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild          |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.959 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable               |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 7.5             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                         |

### Remediation

**Patch Immediately** Patch or fixed version identified

**CISA required action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE      | AFFECTED           | FIXED IN      | SOURCE |
|--------------|--------------------|---------------|--------|
| configurator | ≥ 12.2.3 ≤ 12.2.14 | after 12.2.14 | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-rcj9-qvh8-q3c8](https://github.com/advisories/GHSA-rcj9-qvh8-q3c8)

**Additional guidance** [oracle.com/security-alerts/alert-cve-2025-61884.html](https://oracle.com/security-alerts/alert-cve-2025-61884.html)

**NVD** [nvd.nist.gov/vuln/detail/CVE-2025-61884](https://nvd.nist.gov/vuln/detail/CVE-2025-61884)

**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2025-33878](https://euvd.enisa.europa.eu/vulnerability/EUVD-2025-33878)

**Current data** [evulnable.com/vulnerability-management/cve/CVE-2025-61884](https://evulnable.com/vulnerability-management/cve/CVE-2025-61884)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.