



NCSC-2025-0303

Kwetsbaarheid verholpen in Oracle E-Business Suite

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 08-10-2025

Revisie: 1.0.2

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 2

Aan dit beveiligingsadvies zijn Indicators-of-Compromise toegevoegd. Daarnaast is toegevoegd dat voor de kwetsbaarheid exploitcode in omloop is. Lees de duiding en het handelingsperspectief voor meer informatie.

Feiten

Oracle heeft een zeroday-kwetsbaarheid verholpen in Oracle E-Business Suite (specifiek voor de Concurrent Processing component in versies 12.2.3 tot 12.2.14).

Duiding

De kwetsbaarheid bevindt zich in de Concurrent Processing component van Oracle E-Business Suite (EBS). Ongeauthenticeerde kwaadwillenden kunnen deze kwetsbaarheid misbruiken door malafide HTTP-verzoeken naar het kwetsbare systeem te versturen. Dit kan leiden tot ernstige risico's voor de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. De kwetsbaarheid heeft een CVSS-score van 9.8.

Volgens berichtgeving van Oracle wordt de kwetsbaarheid actief misbruikt. Oracle heeft IOC's beschikbaar gesteld. Beveiligingsbedrijf CrowdStrike heeft aanvullende IOC's gedeeld.

Het NCSC is bekend met exploitcode die in omloop is en waarmee de kwetsbaarheid kan worden misbruikt.

Beveiligingsbedrijf Defuse meldt op X grootschaliger misbruik van de kwetsbaarheid waar te nemen. Het NCSC adviseert om de in dit beveiligingsadvies beschreven maatregelen zo spoedig mogelijk in te zetten en Oracle EBS-systemen op aanwezigheid van de beschikbare IOC's te controleren.

Oplossingen

Installeer de laatste beveiligingsupdates voor Oracle EBS. Op de website van Oracle vind je een overzicht van beschikbare beveiligingsupdates en meer informatie over de updates voor het verhelpen van CVE-2025-61882.

Controleer je Oracle EBS-omgeving op aanwezigheid van de IOC's die door Oracle zijn gedeeld. De kwetsbaarheid werd namelijk al misbruikt voordat Oracle de beveiligingsupdates uitbracht. In het bijzonder organisaties wiens Oracle EBS-omgeving vanaf het internet toegankelijk is, lopen een verhoogd risico te zijn gecompromitteerd. Een overzicht van IOC's vind je in Oracle's advisory. CrowdStrike heeft daarnaast aanvullende IOC's gedeeld.

Controleer je netwerklogs op aanwezigheid van de volgende indicatoren. Aanwezigheid kan duiden op misbruik van de kwetsbaarheid.

- Binnenkomende POST-requests naar de Oracle EBS-server met het URL-pad '/OA_HTML/configurator/UiServlet' en/of '/OA_HTML/SyncServlet'.

- Binnenkomende GET- en/of POST-requests naar '/OA_HTML/RF.jsp' en/of '/OA_HTML/OA.jsp'.
- Binnenkomende GET- en/of POST-requests naar '/OA_HTML/help/' en/of '/OA_HTML/help/./ieshostedsurvey.jsp'. Dit duidt op de mogelijke aanwezigheid van een webshell.
- Binnenkomende en uitgaande GET-requests met 'xsl' in het pad. Dit duidt mogelijk op het downloaden van een malafide xsl-bestand. Een voorbeeld van zo'n pad is '/OA_HTML/OA.jsp?page=/oracle/apps/xdo/oa/template/webui/TemplatePreviewPG&TemplateCode=TMPf2b9b7f8527ad5f5&TemplateType=XSL-TEXT'.
- Uitgaande TCP-verbindingen vanaf je Oracle EBS-server naar onbekende ip-adressen op niet-standaard poorten. Dit wijst mogelijk op misbruik van een reverse shell.

Controleer je Oracle EBS-server ook op aanwezigheid van de volgende indicatoren. Aanwezigheid kan duiden op misbruik van de kwetsbaarheid.

- Verdachte subprocessen onder het primaire Oracle EBS Java-proces. Controleer of het primaire Java-proces een shell als subprocess genereert.
- De uitvoer van verdachte shell-commando's. Op Linux zijn dit bijvoorbeeld 'sh -c', 'bash -i' en commando's die refereren naar '/dev/tcp/'. Op Windows gaat het bijvoorbeeld om 'cmd /c' en 'powershell.exe' met encoded commando's.
- Aanwezigheid van het bestand 'Log4jConfigQpgsubFilter.java' met de hash dfaed679bda45b73689559a8eba8633b. Dit is een backdoor die door de actor wordt geplaatst.

Referenties

- <https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-cve-2025-61882/>
- <https://www.oracle.com/security-alerts/alert-cve-2025-61882.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-61882	9.3 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-287	Improper Authentication

Getroffen producten

Oracle
Concurrent Processing

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.