INTEGRIGY

May 20, 2022

Oracle E-Business Suite Security Analysis

CVE-2022-21500 Analysis and Recommendations

Vulnerability Overview

Oracle has released an out-of-cycle security alert for Oracle E-Business Suite (EBS) to address an information disclosure security vulnerability. **The vulnerability is being actively exploited in externally accessible Oracle EBS environments running modules such as iSupplier, iStore, iRecruitment, and iSupport.** This vulnerability is exploitable in all Oracle EBS versions including 12.0 and 11.5 even though these versions are not listed in the Oracle advisory.

This vulnerability may allow an unauthenticated user to view all the Oracle EBS users through the application Manage Proxies page, which **displays username, first name, last name, and e-mail address** in a list of values (LOV). In order to exploit this vulnerability, the attacker must first register an account with Oracle EBS using one of the self-registration capabilities within the application. By default, the Manage Proxies is available to new users unless explicitly removed, such as with iSupplier and other external modules. However, if an attacker is able to register a new user that does not grant any responsibilities, the Manage Proxies feature will be available to the user. Within iStore there is such a registration page that is available even though iStore may not be installed, licensed, or configured.

This risk of this vulnerability is primarily for externally exposed Oracle EBS environments running external modules such as iSupplier, iStore, iRecruitment, iSupport, etc. If the external DMZ environment is not correctly configured and blocks unused modules using a security solution such as Integrigy AppDefend or the Oracle EBS URL Firewall, then the environment is most likely vulnerable to this issue.

Internally, this vulnerability is exploitable, however, most likely an internal user or attacker with access to Oracle EBS internally will be able to obtain this first name, last name, and e-mail address from multiple other sources. Of most concern internally will be access to customer, supplier, and job candidate names and e-mail addresses when using iSupplier, iStore, iRecruitment, etc. Detailed information on this vulnerability has been published and the published attack vector is the iStore self-registration page /OA_HTML/ibeCAcpSSOReg.jsp.

VULNERABILITY VALIDATION

To validate if your environment is exploitable, all the following conditions must be satisfied –

1. The ibeCAcpSSOReg.jsp page is accessible, with the most risk being external environments. Attempt to access the following page both internally and externally. If iStore is not used and Integrigy AppDefend is used or the Oracle EBS URL Firewall is properly configured, then this page should not be accessible with the message "403 Forbidden" or "410 Gone". Internally, if Oracle EBS Allowed Resources is correctly configured, then this page should not be accessible with the error message "Requested resource or page is not allowed in this site".

   ```
   https://<site>/OA_HTML/ibeCAcpSSOReg.jsp
   ```

2. Self-registration is configured in iStore, which is the default. If it is not enabled, then you will receive the error message "User self registration has been disabled in the system." when accessing the above page. Self-registration is configured using the System Profile Option "APPS_SSO_USER_CREATE_UPDATE" and is set to "Y" to enable self-registration.

3. Proxy Delegation Privilege is set to "All Users" rather than a list of specific roles or responsibilities. This can be verified by accessing in Oracle E-Business Suite the User Management responsibility > Proxy Configuration page > Privileges tab. Depending on your Oracle E-Business Suite version and patch levels, the Proxy Configuration function may not be available in which case the setting is "All Users".

VULNERABILITY PROTECTION

Existing recommendations, web application firewalls, and other security products that block access to the ibeCAcpSSOReg.jsp page are NOT effective as this is not one of the vulnerable pages but just a landing page that is used to access the actual vulnerable registration pages.

Integrigy AppDefend

Integrigy AppDefend will block access to the vulnerable iStore pages externally unless iStore (IBE) is configured as part of the OA Permit oebs-modules-allow group. Internally, if the OA Permit oebs-modules-allow group is configured with a list of modules, the vulnerable iStore page will be blocked. If the OA Permit oebs-modules-allow group is set as "All" either internally or externally, then the vulnerable page is accessible. An AppDefend update is available that specifically blocks access to the vulnerable pages.

URL Firewall and Allowed Resources

The vulnerable pages may be blocked by the Oracle E-Business Suite DMZ URL Firewall externally or the Allowed Resources if correctly configured to block iStore pages.

Disable Manage Proxies

The Manage Proxies functionality can be restricted to only specific roles and responsibilities. Change the Proxy Delegation Privilege from “All Users” to a list of specific responsibilities. This is accessed through the User Management responsibility > Proxy Configuration page > Privileges tab. Depending on your Oracle E-Business Suite version and patch levels, the Proxy Configuration feature may not be available in which case the setting is “All Users”.

Disable User Registration

User registration can be disabled by setting the System Profile Option “APPS_SSO_USER_CREATE_UPDATE” to “N” at the site level. This will disable self-registration for both iStore and iRecruitment. Be sure to verify self-registration is not required for either iStore or iRecruitment prior to changing this setting.

Custom iStore Pages

If you are using iStore, it is common to customize iStore pages to update the look and feel for your organization. This is done by copying the standard Oracle iStore pages to custom pages that are prefixed with an identifier such as “xx” and your organization’s custom application identifier. Review any iStore customizations to determine if the pages ibeCAcpSSOReg.jsp or ibeCRgp* were customized and include these pages in any remediation steps.

Oracle EBS Patch

Oracle intends to release a patch to correct this vulnerability on June 15th. Most likely, the functionality of the Manage Proxies will be changed to prevent self-registration users from accessing the Manage Proxies.

VULNERABILITY EXPLOITATION DETECTION

To detect if this vulnerability has been exploited in your environment, you should check (1) if the vulnerable web pages have been accessed and (2) if users have been self-registered. There is no reliable method to determine what user information was accessed through the exploitation of this vulnerability.

1. Review the Oracle HTTP Server access logs to see if the following pages have been accessed recently –

   ```
   /OA_HTML/ibeCAcpSSOReg.jsp
   /OA_HTML/ibeCRgpIndividualUser.jsp
   /OA_HTML/ibeCRgpPrimaryCreate.jsp
   /OA_HTML/ibeCRgpPartnerPriCreate.jsp
   ```

   Oracle HTTP Server access logs are in the following directory depending on Oracle EBS version. Be aware that these files are rotated, so multiple files may have to be checked.

   ```
   12.2 = $RUN_TOP/FMW_Home/Oracle_EBS-app1/applications/oacore/html
   12.1/12.0 = $INST_TOP/apps/<SID>_<HOST>/logs/ora/10.1.3/Apache
   11.5.10 = $IAS_ORACLE_HOME/Apache/Apache/logs
   ```

2. Use the following SQL to find any users that may have been created through the self-registration process. End-date the users if determined to be maliciously created.

   ```
   select R.USER_ID, R.CREATION_DATE, U.USER_NAME, U.EMAIL_ADDRESS
   from JTF.JTF_UM_USERTYPE_REG R, APPLSYS.FND_USER U
   where R.USER_ID = U.USER_ID
   and R.STATUS_CODE = 'APPROVED'
   and R.CREATED_BY = 6
   order by CREATION_DATE desc;
   ```

3. If malicious users have been identified, then review the access logs to see if the LOV page below has been accessed. This page will be accessed as part of standard application functionality, so you must correlate the access with the above pages to determine which access may have been malicious. This will only indicate the number of times the LOV was accessed and not the actual data viewed by the attacker unless the attacker entered a filter in the LOV popup.

   ```
   OA.jsp?region=/oracle/apps/fnd/umx/lov/webui/ProxyUsersLOVRN
   ```

ORACLE EBS SECURITY RECOMMENDATIONS

Considering this vulnerability disclosure and likely increase in Oracle EBS attacks as well as disclosure of other Oracle EBS security vulnerabilities, proactive steps should be taken to secure all external Oracle environments to limit the risk to the environment. In addition to the recommendations in the Oracle EBS Secure Configuration Guide, the following security recommendations should be implemented for all Oracle EBS environments –

1. Use AppDefend to protect your Oracle EBS through virtual patching of Oracle EBS security bugs fixed as part of the Critical Patch Updates and blocking classes of security vulnerability like SQL injection, cross-site scripting, Java deserialization, and XML entity attacks. AppDefend reduces the surface area of the Oracle EBS externally to only those application modules and web pages required.

2. Ensure FND_DIAGNOSTICS is not enabled in the environment. This can be determined by periodically checking, such as with an Oracle Alert, the System Profile Option FND_DIAGNOSTICS at the site, application, organization, responsibility, and server level. Under no circumstances should FND_DIAGNOSTICS ever be enabled except at the user level for trusted, privileged users. If enabled, an attacker or user is able to execute arbitrary SQL queries using the APPS database account. AppDefend blocks access to FND_DIAGNOSTICS except of explicitly allowed users.

3. Implement single sign-on (SSO) and multifactor authentication (MFA) for Oracle EBS using AppDefend, which is a rapid to implement and cost-effective solution compared to other Oracle EBS SSO solutions. AppDefend SSO and MFA can help to eliminate malicious access to the application and provide an additional layer of security for external Oracle EBS modules like iSupplier.

4. External DMZ Oracle EBS environments must have the URL Firewall enabled and correctly configured in order to prevent exploitation of vulnerabilities such as this one and to reduce the surface area of the application. Internal environments should have the Allowed Resources feature enabled and configured for only the modules used in your environment.

Integrigy will be presenting an educational webinar, "CVE-2022-21500: Why Did a 100 Hackers Just Attack My Oracle E-Business Suite Environment", on Monday, May 23rd at 2 pm EDT. A recording of this webinar will be available after the webinar on our YouTube channel at https://youtube.com/integrigy. Please contact Integrigy at info@integrigy.com if you would like additional information or need assistance with remediating the impact of this vulnerability.

References

- Oracle Security Alert Advisory - CVE-2022-21500, 19 May 2022, https://www.oracle.com/security-alerts/alert-cve-2022-21500.html
- Security Alert CVE-2022-21500 Patch Availability Document for Oracle E-Business Suite, 19 May 2022, My Oracle Support Note ID 870472.1

History

May 19, 2022 – Initial Internal Analysis
May 20, 2022 – AppDefend and AppSentry Updated
May 20, 2022 – Published version 1

About Integrigy

Integrigy Corporation is a leader in application security for enterprise mission-critical applications and databases. AppSentry, our ERP application and database security assessment tool, assists companies in securing their largest and most important applications and databases through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite and PeopleSoft. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

Integrigy Corporation
14 Westlake Drive
Nashville, Tennessee 37205 USA
888/542-4802
www.integrigy.com

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernible. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.