CVE-2022-21500
Why Did a 100 Hackers Just Attack My Oracle E-Business Suite Environment

May 23, 2022

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications

Oracle E-Business Suite
and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database
Security Auditing Tool

Validates and Audits Security

AppDefend

Enterprise Application Firewall
for Oracle E-Business Suite
and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

Vulnerability Exploit Requirements #1

- **ibeCAcpSSOReg.jsp and vulnerable pages are accessible**
  - The most risk is external environments
  - Attempt to access the following page both internally and externally

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

- **If a valid page or the Oracle EBS Error page is displayed for any of above pages, the environment is vulnerable**
- **If any of the following are displayed, the environment is not vulnerable –**
  - AppDefend = “403 Forbidden”
  - URL Firewall = “410 Gone”
  - Allowed Resources = “Requested resource or page is not allowed in this site”
  - Other messages may be displayed if blocked by web application firewalls, …

Vulnerability Exploit Requirements #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 iStore landing page**
- **Self-registration is configured using the System Profile Option "APPS_SSO_USER_CREATE_UPDATE"**
  - Set to "Y" to enable self registration or "N" to disable
- **Proxy Delegation Privilege is set to "All Users" rather than a list of specific roles or responsibilities**
  - Access 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 #1

- **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
- **URL Firewall and Allowed Resources if correctly configured**
  - Externally, use Oracle EBS DMZ URL Firewall to block the vulnerable pages
  - Internally, user Allowed Resources to block the vulnerable 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
  - 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”

Vulnerability Protection #2

- **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 Detection – Access Logs

- **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 –**
  - Depends 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/user_projects/domains/EBS_domain/servers/oacore_server1/logs
12.1/12.0 = $INST_TOP/apps/<SID>_<HOST>/logs/ora/10.1.3/Apache
11.5.10 = $IAS_ORACLE_HOME/Apache/Apache/logs
```

Vulnerability Detection – Created Users

- Check for self-registration users
  - 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;
```

Vulnerability Detection – Data Accessed

- If malicious users have been identified –
  - 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

- Use AppDefend to protect your Oracle EBS
  - **Virtual patching** of Oracle EBS security bugs fixed as part of the Critical Patch Updates
  - **Blocking classes of security vulnerability** like SQL injection, cross-site scripting, Java deserialization, and XML entity attacks
  - **Reduces the surface** area of the Oracle EBS externally to only those application modules and web pages required
  - **Single Sign-on** (SSO) and **Multifactor Authentication** (MFA)

- Ensure **FND_DIAGNOSTICS** is not enabled in the environment.
  - Periodically check, 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 execute arbitrary SQL queries using the APPS database account

Oracle EBS Security Recommendations

- Implement single sign-on (SSO) and multifactor authentication (MFA)
  - Use AppDefend, which is a rapid to implement and cost-effective solution compared to other Oracle EBS SSO solutions
  - Eliminate malicious access to the application and provide an additional layer of security for external Oracle EBS modules like iSupplier
- External DMZ Oracle EBS environments must have the URL Firewall enabled
  - Must be correctly configured in order to prevent exploitation of vulnerabilities
  - Reduce the surface area of the application
- Internal environments should have the Allowed Resources feature enabled
  - Must be correctly configured for only the modules used in your environment

CVE-2022-21500 References

- **Integrigy CVE-2022-21500 Analysis and Recommendations**
  - https://www.integrigy.com/security-resources/cve-2022-21500-analysis-and-recommendations
- **Oracle Security Advisory**
  - https://www.oracle.com/security-alerts/alert-cve-2022-21500.html
- **Original Published Vulnerability and Exploit**
  - https://orwaatyat.medium.com/my-new-discovery-in-oracle-e-business-login-panel-that-allowed-to-access-for-all-employees-ed0ec4cad7ac
- **Shodon.io**
  - https://www.shodan.io/search?query=%22X-ORACLE-DMS-ECID%22+http.title%3A%22Login%22+200
- **Google Dork**
  - https://www.google.com/search?q=inurl:OA_HTML

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**

linkedin – **linkedin.com/company/integrigy**

twitter – **twitter.com/integrigy**