SYNACKTIV
DIGITAL SECURITY

# Unauthenticated log files leak 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 log files without being authenticated.

The *Enterprise Communications Broker* Web administration console does not verify if the user is authenticated when accessing exported log files.

## 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-2016-3515 / S0691314 |

# Technical description and Proof-of-Concept

## Vulnerability discovery

The files exposed in the URL */webapps/export/** are accessible for unauthenticated users.

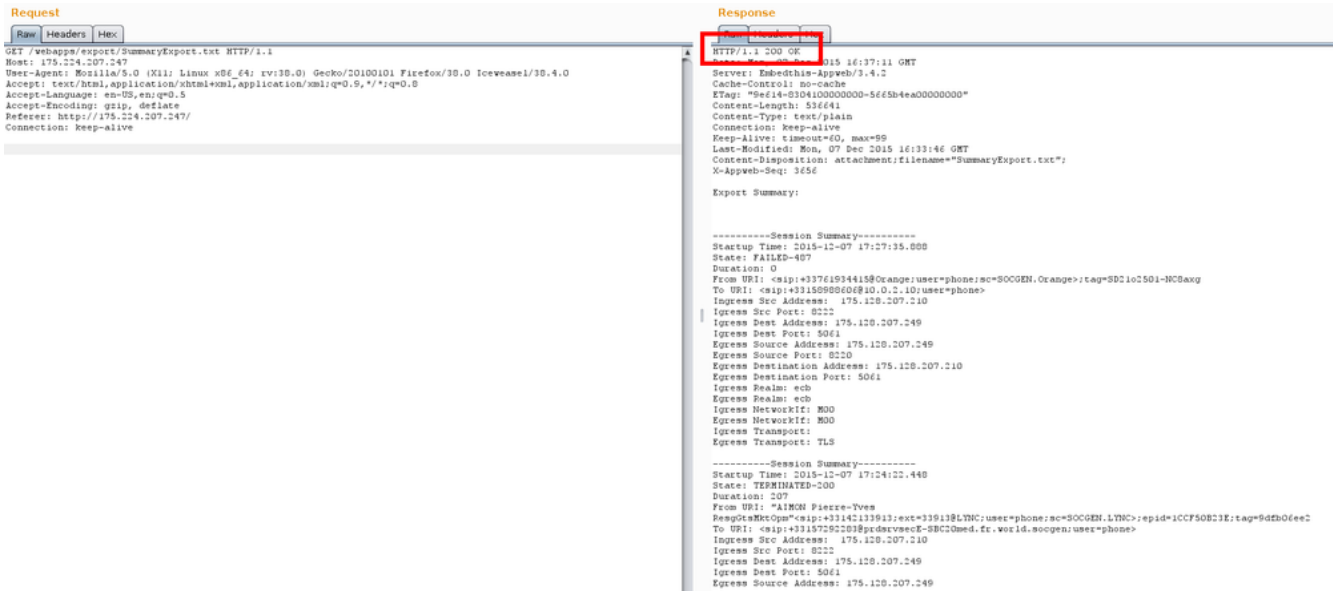


Illustration 1: Accessing a SIP sessions summary without being authenticated

When access control checks are not applied, users are able to access data or perform actions that they should not be allowed to perform.

It allows an attacker to:

- understand many technical details related to the VoIP infrastructure,
- list previously made and on-going calls including the identity of callers and callees.