SYNACKTIV
DIGITAL SECURITY

Configuration issues in Oracle Enterprise Communications Broker & Monitor

Security advisory

01/02/2016

Nicolas Collignon
Sébastien Dudek

Issues 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 Oracle Enterprise Communications Monitor

The Oracle Enterprise Communication Monitor allows to capture and analyze the signaling messages. It provides a better visibility of the exchange made before establishing a call and allows an end-to-end call correlation and quality metrics.

The issues

Synacktiv has identified two configuration issues to fix respectively in Oracle Enterprise Communication Broker and Oracle Enterprise Communication Monitor.

1. Session cookies not marked Secure and HttpOnly in Oracle Enterprise Communication Monitor

Session cookies used by the Web application Oracle *Communications Operations Monitor* are not marked with the security attributes *Secure* and *HttpOnly*.

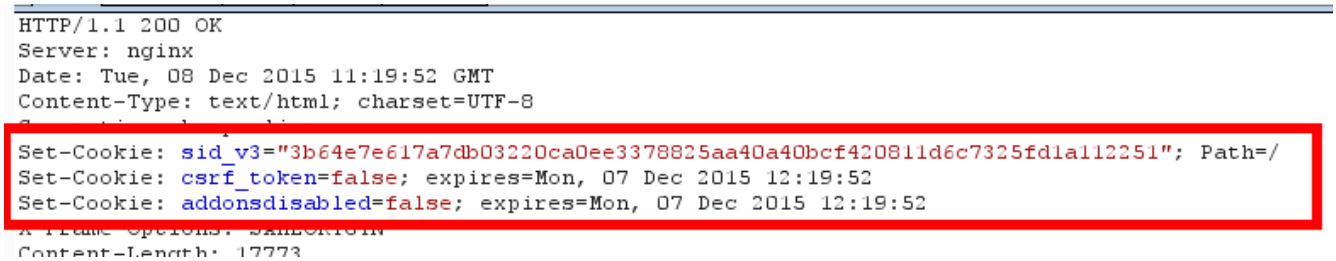

Illustration 1: Cookies defined without security attributes by the Communications Operations Monitor Web application

Without the attribute *secure*, the session cookies can transit in an insecure communication (HTTP) despite the HTTP to HTTPS redirection.

Illustration 2: Leak of the session identifier and anti-CSRF token on an insecure HTTP channel

The attribute *HttpOnly* attribute prevents cookies' manipulation by local scripts such as JavaScript. It makes Cross-Site Scripting (XSS) attacks more complex to exploit.

Affected versions

The following versions are affected:

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

2. Banner leak in HTTP headers in Oracle Enterprise Communication Broker

The *Oracle Communications Broker* web server leaks the name and the version of the HTTP server implementation.

```
HTTP/1.1 200 OK
Date: Tue, 08 Dec 2015 10:45:26 GMT
Server: Embedthis-Appweb/3.4.2
[...]
```

By analyzing the banners, an attacker could determine which application or technology is used by the company. If the attacker can get the exact version of an application or of a framework, he could know if it is publicly known as vulnerable. A hacker getting several technical data will orientate its further attacks focusing on the applications used.

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-2016-3513 / S0687566 Vulnerability fixed in Oracle *Critical Patch Update* July 2016 / CVE-2016-3514 / S0687668