Missing update in Oracle Enterprise Communications Broker web server

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

The Oracle Enterprise Communications Broker embedded Web server is currently an Embedthis-Appweb version 3.4.2. This version is affected by several vulnerabilities including CVE-2014-9708. The current Appweb sources is the version 5 with long term support.

If updates are not performed, an attacker could use exploit codes, sometimes freely accessible on the Internet, to compromise the server.

It is shown that version 4 is vulnerable to a null pointer dereference, referenced as CVE-2014-9708, due to incorrect parsing of HTTP headers (https://github.com/embedthis/appweb/issues/413). The version 3.4.2 is also vulnerable according to the sources at URL: http://embedthis.com/software/appweb-3.4.2-0-src.tgz.

Indeed, an analysis of the sources of the parseRange() function in appweb/appweb-3.4.2/src/http/request.c, show the function does not mitigate a null range following with a coma at line 1120:

```c
/*
 * A range "-7" will set the start to -1 and end to 8
 */
tok = mprStrTok(value, ",", &value);
if (*tok != '-') {
    range->start = (int) mprAtoi(tok, 10);
} else {
    range->start = -1;
}
range->end = -1;
```

An attacker can send a crafted request to crash the server as follows:

```
GET / HTTP/1.0
Range: x=,
```

Affected versions

The following versions are affected:

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

Mitigation

Install Oracle Critical Patch Update July 2016.
<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/02/2016</td>
<td>Advisory sent to Oracle Security.</td>
</tr>
<tr>
<td>19/07/2016</td>
<td>Vulnerability fixed in Oracle <em>Critical Patch Update</em> July 2016 / CVE-2014-9708 / S0688016</td>
</tr>
</tbody>
</table>