MWR InfoSecurity Security Advisory

OpenSC - “Get Serial Number” Stack-based Buffer Overflow

13th December 2010
OpenSC – “Get Serial Number” Stack-based Buffer Overflow

<table>
<thead>
<tr>
<th>Package Name:</th>
<th>OpenSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Reported</td>
<td>3rd November 2010</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>Confirmed in Version 0.11.13 and earlier</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVE Reference</th>
<th>Not Yet Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Rafael Dominguez Vega</td>
</tr>
<tr>
<td>Severity</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>Vulnerability Class</td>
<td>Stack-based buffer overflow</td>
</tr>
<tr>
<td>Vendor</td>
<td>OpenSC - <a href="http://www.opensc-project.org">http://www.opensc-project.org</a></td>
</tr>
<tr>
<td>Vendor Response</td>
<td>The vendor has implemented a fix. <a href="https://www.opensc-project.org/opensc/changeset/4913">https://www.opensc-project.org/opensc/changeset/4913</a></td>
</tr>
<tr>
<td>Exploit Details Included</td>
<td>No</td>
</tr>
</tbody>
</table>

Overview

MWR InfoSecurity identified a vulnerability in OpenSC. The vulnerability can be triggered using a malicious smart card.

Impact

An attacker could use this vulnerability to execute arbitrary code in the target system. To successfully exploit this vulnerability the attacker will be required to insert a specially crafted smart card in the target system.

Cause

A buffer overflow vulnerability was identified in the code handling the smart card’s serial number in the following drivers:

- card-atrust-acos.c
- card-acos5.c
- card-starcos.c

Interim Workaround

The interim workaround for this issue will require the affected drivers to be removed from OpenSC and this to be recompiled.

Solution

The vendor has implemented a fix. Users should upgrade to the latest version of OpenSC. [https://www.opensc-project.org/opensc/changeset/4913](https://www.opensc-project.org/opensc/changeset/4913)

Dependencies

In order to successfully exploit the vulnerability described in this advisory, an attacker would
need to have physical access to the affected system in order to be able to plug in a malicious smart card.

**Detailed Vulnerability Description**

The issue is a stack-based buffer overflow affecting the following drivers, in the "Get Serial Number" function.

- card-atrust-acos.c
- card-acos5.c
- card-starcos.c

The affected code is included here. The vulnerability is in the `memcpy` shown below, as the serial number that the card sends can be larger (up to 258 bytes) than the buffer where the data is being copied to (32 bytes).

```c
#define SC_MAX_SERIALNR 32
#define SC_MAX_APDU_BUFFER_SIZE 258

u8 rbuf[SC_MAX_APDU_BUFFER_SIZE];
...
apdu.resp = rbuf;
apdu.resplen = sizeof(rbuf);
...
memcpy(card->serialnr.value, apdu.resp, apdu.resplen);
```

During the investigation of this vulnerability a Proof-of-Concept smart-card was created. The malicious smart card was specially developed to trigger this issue and overwrite the value of the instruction pointer.
Acknowledgement

Thanks to Nils for the support and guidance on this research.

Thanks to Martin Paljak of OpenSC for his co-operation in working with the author in regards to this matter and acknowledge his prompt response in implementing a fix.