

MWR InfoSecurity Security
Advisory

PCSC-Lite:
libccid Buffer Overflow

13th December 2010

MWR  INFOSECURITY

PCSC - libccid Buffer Overflow Vulnerability

Package Name:	PCSC-Lite
Date Reported	3 rd November 2010
Affected Versions:	Confirmed in Version 1.5.3

CVE Reference	Not Yet Assigned
Author	Rafael Dominguez Vega
Severity	Medium Risk
Vulnerability Class	Buffer overflow
Vendor	PCSC-Lite - http://pcslite.alioth.debian.org/
Vendor Response	The vendor has implemented a fix. http://lists.alioth.debian.org/pipermail/pcslite-cvs-commit/2010-November/004934.html http://lists.alioth.debian.org/pipermail/pcslite-cvs-commit/2010-November/004935.html
Exploit Details Included	No

Overview

MWR InfoSecurity identified a vulnerability in PCSC-Lite's pcsd daemon. 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 malicious smart card reader in the target system.

Cause

A buffer overflow vulnerability was identified in the code handling the communication of the serial port smart card reader (ccid_serial.c). The vulnerability occurs as the value of the length supplied in the affected memcopy can be negative, and consequently larger than the destination buffer.

Interim Workaround

Disabling the pcsd daemon will prevent users from exploiting the vulnerability.

Solution

The vendor has implemented a fix. Users should upgrade to the latest version of PCSC-Lite.
<http://lists.alioth.debian.org/pipermail/pcslite-cvs-commit/2010-November/004934.html>
<http://lists.alioth.debian.org/pipermail/pcslite-cvs-commit/2010-November/004935.html>

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 reader.

Detailed Vulnerability Description

The issue is a buffer overflow affecting the code responsible for handling the communication of the serial port smart card reader (ccid_serial.c).

The affected code is included here. The vulnerability is in the memcpy shown below, as a negative value can be passed to "length" in the memcpy.

The value of "to_read" is incoming data from the reader, which is passed to the "get_bytes" functions and then is used as the length to be copied in the affected memcpy. A negative value passed in the memcpy as the length is larger than the destination buffer, consequently causing the buffer to overflow.

```
to_read = 10+dw2i(buffer, 1);
...
if ((rv = get_bytes(reader_index, buffer+5, to_read-5)) != STATUS_SUCCESS) return
rv;

...

int get_bytes(unsigned int reader_index, unsigned char *buffer, int length)
{
...
    if (offset + length <= offset last) {
        memcpy(buffer, serialDevice[reader_index].buffer + offset, length)
    }
}
```

Source code from ccid_serial.c

Acknowledgement

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

Thanks to Ludovic Rousseau for his co-operation in working with the author in regards to this matter and acknowledge his prompt response in implementing a fix.

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com