DefenseCode

IBM DB2 Command Line Processor Buffer Overflow

IBM DB2 Command Line Processor Buffer Overflow	
Advisory ID:	**DC-2017-04-002**
Software:	**IBM DB2**
Version:	**V9.7, V10.1, V10.5, V11.1**
Vendor Status:	**Contacted / Fixed (CVE-2017-1297)**
Release Date:	**26.06.2017**
Risk:	**High**

1. General Overview

IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) Command Line Process (CLP) is vulnerable to a stack based buffer overflow, caused by improper bounds checking which could allow an attacker to execute arbitrary code. The vulnerability is triggered by providing an overly long procedure name inside a CALL statement.

2. Software Overview

DB2 is a database product from IBM. It is a Relational Database Management System. DB2 is designed to store, analyze and retrieve the data efficiently. DB2 currently supports Linux, UNIX and Windows platforms.

db2bp is a persistent background process for the DB2 Command Line Processor, and it is the process which actually connects to the database.

3. Brief Vulnerability Description

By providing a specially crafted command file to the db2 CLP utility, it is possible to cause a buffer overflow and possibly hijack the execution flow of the program. Crafted file contains a CALL statement with an overly long procedure parameter.

3.1 Proof of Concept

The following python script will generate a proof of concept .sql crash test file that can be used to verify the vulnerability:

```
#!/usr/bin/python

load_overflow = 'A' * 1000
statement = "CALL " + load_overflow + ";"

crash_file = open("crash.sql", "w")
crash_file.write(statement)
crash_file.close()
```

PoC usage: ***db2 -f crash.sql***

4. Solution

The recommended solution is to apply the appropriate fix for this vulnerability. More details on: http://www-01.ibm.com/support/docview.wss?uid=swg22004878

5. Credits

Vulnerability discovered by Leon Juranic, further analysis by Bosko Stankovic.

6. Disclosure Timeline

04/04/2017	**Vendor contacted**
04/12/2017	**Vulnerability assessed and acknowledged by vendor**
06/22/2017	**Vulnerability fixed and advisory published by vendor (CVE-2017-1297)**
06/26/2017	**Advisory published by DefenseCode**

7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/