



SA28074 / CVE-2008-0067

Generated by Secunia

7 January, 2009

4 pages

Table of Contents

Introduction	2
Technical Details	2
Exploitation	3
Characteristics	3
Tested Versions	4
Fixed Versions	4
References	4

Introduction:

=====

A vulnerability in the OpenView5.exe CGI application in HP OpenView Network Node Manager can be exploited to cause a stack-based buffer overflow and compromise a vulnerable system.

Technical Details:

=====

HP OpenView Network Node Manager provides access to certain CGI applications via the following URI:

http://[host]/OvCgi/[CGI_application]

A boundary error within the OpenView5.exe CGI application when handling strings passed to the "Context" parameter with the "Help" parameter set to an arbitrary string can be exploited to cause a stack-based buffer overflow.

OpenView5.exe first retrieves the strings assigned to the various parameters (some disassembly not shown).

```
.text:00401000 ; int __cdecl main(int argc, const char **argv, const char *envp)
.text:00401000 _main      proc near          ; CODE XREF: start+DEp
.text:00401000
.text:00401000 var_A7C      = dword ptr -0A7Ch
.text:00401000 var_A78      = dword ptr -0A78h
...
.text:00401000 param_Target = dword ptr -0A4Ch
.text:00401000 param_HelpWin = dword ptr -0A48h
...
.text:00401000 param_NoFrames = dword ptr -0A3Ch
...
.text:00401000 param_Map      = dword ptr -0A30h
...
.text:00401000 param_Session = dword ptr -0A28h
.text:00401000 param_Context = dword ptr -0A24h
.text:00401000 param_Action = dword ptr -0A20h
...
.text:00401000 param_Title  = dword ptr -0A14h
...
.text:00401000 var_4        = byte ptr -4
.text:00401000 argc          = dword ptr 8
.text:00401000 argv          = dword ptr 0Ch
.text:00401000 envp          = dword ptr 10h
.text:00401000
.text:00401000      push    ebp
.text:00401001      mov     ebp, esp
.text:00401003      sub     esp, 0A7Ch
.text:00401009      push    esi
.text:0040100A      mov     [ebp+var_A2C], 1E13380h
.text:00401014      mov     [ebp+var_A34], offset aHostOid_iso_or ; "&Host=&Oid=.iso.org.dod.internet&Commun"...
.text:0040101E      lea    ecx, [ebp+var_4]
.text:00401021      call   ds:??0cgiEntries@@QAE@XZ ; cgiEntries::cgiEntries(void)
.text:00401027      push    offset aContext ; "Context"
.text:0040102C      lea    ecx, [ebp+var_4]
.text:0040102F      call   ds:?find@cgiEntries@@QBEPBDPBD@Z ; cgiEntries::find(char const *)
.text:00401035      mov     [ebp+param_Context], eax
.text:0040103B      push    offset aAction ; "Action"
...
```

Execution eventually reaches loc_401578, which retrieves the number of parameters used in the request and if it is not zero, checks if the "Target" parameter is assigned a string.

```
.text:00401578 loc_401578:          ; CODE XREF: _main+557j
.text:00401578          ; _main+560j
.text:00401578      lea    ecx, [ebp+var_4]
.text:0040157B      call   ds:?count@cgiEntries@@QBEXXZ ; cgiEntries::count(void)
.text:00401581      test   eax, eax
```

```
.text:00401583          jz      loc_401896
.text:00401589          mov     [ebp+var_A6C], offset unk_40331C
.text:00401593          push   offset aTarget_0 ; "Target"
.text:00401598          lea    ecx, [ebp+var_4]
.text:0040159B          call   ds:?find@cgiEntries@@QBEPBDPBD@Z ; cgiEntries::find(char const *)
.text:004015A1          mov     [ebp+param_Var], eax
.text:004015A7          cmp    [ebp+param_Var], 0
.text:004015AE          jz     loc_401761      ; no string assigned to "Target"?
```

If no string is assigned to the "Target" parameter, another check is done for the "Help" parameter.

```
.text:00401761 loc_401761:          ; CODE XREF: _main+5AEj
.text:00401761          push   offset aHelp    ; "Help"
.text:00401766          lea    ecx, [ebp+var_4]
.text:00401769          call   ds:?find@cgiEntries@@QBEPBDPBD@Z ; cgiEntries::find(char const *)
.text:0040176F          mov     [ebp+param_Var], eax
.text:00401775          cmp    [ebp+param_Var], 0
.text:0040177C          jz     short loc_4017DB ; no string assigned to "Help"?
```

If a string is assigned to the "Help" parameter, the string `"/OvCgi/OvHelp.exe?Context=<Context parameter string>"` is created into a 512-byte stack buffer with no bounds checking. This may cause a stack-based buffer overflow.

```
.text:0040177E          push   offset aOvcgiOvhelp_ex ; "/OvCgi/OvHelp.exe"
.text:00401783          lea    eax, [ebp+var_A10] ; char[512]
.text:00401789          push   eax
.text:0040178A          call   ds:strcpy_new
.text:00401790          add    esp, 8
.text:00401793          push   offset a?context ; "?Context="
.text:00401798          lea    ecx, [ebp+var_A10] ; char[512]
.text:0040179E          push   ecx
.text:0040179F          call   ds:strcat_new
.text:004017A5          add    esp, 8
.text:004017A8          mov    edx, [ebp+param_Context]
.text:004017AE          push   edx
.text:004017AF          lea    eax, [ebp+var_A10] ; char[512]
.text:004017B5          push   eax
.text:004017B6          call   ds:strcat_new
```

Exploitation:

=====

Exploitation is straight-forward by sending e.g. a POST request to the OpenView5.exe CGI application with the "Help" parameter set to an arbitrary string and the "Context" parameter set to an overly long string to overwrite the return address or a structured exception handler.

Secunia Research has developed both a PoC and working exploit for the vulnerability. These are available to customers via the BA customer web interface.

Characteristics:

=====

Detection:

Look for HTTP requests to the OpenView5.exe CGI application and check if:

- * the "Help" parameter is assigned an arbitrary string
- * the "Context" parameter is assigned an overly long string such that the created string `"/OvCgi/OvHelp.exe?Context=<Context parameter string>"` is greater than or equal to 512 bytes.

Verification:

A way to easily verify the vulnerability without a debugger has not been found as the vulnerability lies in a CGI application, which is executed by e.g. the inetinfo.exe service in Windows XP and terminates with no warnings if the said CGI application crashes.

Identification:

The vulnerability is confirmed in OpenView5.exe (no version information available) as included in HP OpenView Network Node Manager version 7.51, but other versions may also be affected. The default installation location is "%ProgramFiles%\HP OpenView\www\cgi-bin".

Tested Versions:

=====

The vulnerability was analysed on Windows XP SP2 running HP OpenView Network Node Manager version 7.51 with patch NNM_01168 applied, and incorporating OpenView5.exe with an MD5 sum of 25617b70balcf56721fd361b3a0aba52.

Fixed Versions:

=====

The vulnerability is currently unpatched.

References:

=====

SA28074#1:

<http://secunia.com/advisories/28074/>

CVE-2008-0067:

http://secunia.com/cve_reference/CVE-2008-0067/

Secunia Research:

http://secunia.com/secunia_research/2008-4/