CYBSEC S.A.
www.cybsec.com

Advisory Name: SAP Internet Graphics Service (IGS) Remote Buffer Overflow

Vulnerability Class: Heap Buffer Overflow

Release Date: 2007-01-18

Affected Applications:
- SAP IGS 6.40 Patchlevel ≤ 15
- SAP IGS 7.00 Patchlevel ≤ 3

Affected Platforms:
- AIX 64 bits
- HP-UX on IA64 64bit
- HP-UX on PA-RISC 64bit
- Linux on IA32 32bit
- Linux on IA64 64bit
- Linux on Power 64bit
- Linux on x86_64 64bit
- Linux on zSeries 64bit
- OS/400 V5R2M0
- Solaris on SPARC 64bit
- TRU64 64bit
- Windows Server on IA32 32bit
- Windows Server on IA64 64bit
- Windows Server on x64 64bit

Local / Remote: Remote

Severity: High

Author: Mariano Nuñez Di Croce

Vendor Status:
- Confirmed. Updates Released.

Reference to Vulnerability Disclosure Policy:
http://www.cybsec.com/vulnerability_policy.pdf

Product Overview:

"The IGS provides a server architecture where data from an SAP System or other sources can be used to generate graphical or non-graphical output."

It is important to note that IGS is installed and activated *by default* with the Web Application Server (versions ≥ 6.30)

Vulnerability Description:

A specially crafted HTTP request can trigger a remote buffer overflow in SAP IGS service.

Technical Details:

The *ADM:GETLOGFILE* command receives a *portwatcher* as a parameter. If the specified *portwatcher* is not found, an error message is returned to the client.

The vulnerability specifically exists in the processing of this error message.
The message is build by the use of the *_snprintf()* function, which helps to prevent the occurrence of buffer overflows by limiting the number of bytes written to the destination buffer:

```
8B5424 14        MOV EDX,DWORD PTR SS:[ESP+14]   ; Portwatcher string (controlled)
52               PUSH EDX
68 B49C5700      PUSH igsmux.00579CB4    ; ASCII "Could not find portwatcher %s"
8D8424 B0000000  LEA EAX,DWORD PTR SS:[ESP+B0]   ; Destination buffer
68 00040000      PUSH 400                        ; Output 1024 bytes max
50               PUSH EAX
E8 DA881100      CALL <JMP.&MSVCR71._snprintf>
```

Therefore, if a parameter of more than 998 bytes is received, only the first 1024 bytes of the resulting string (after concatenation) would be stored in the destination buffer and no overflow would occur.

To present this error message to the client, an HTTP response is crafted. Its content is prepared in a buffer stored in the heap. After some procedures, the error message string is copied to this buffer:

```
8B4D 0C          MOV ECX,DWORD PTR SS:[EBP+C]  ; _snprintf() result value
8B75 08          MOV ESI,DWORD PTR SS:[EBP+8]  ; Error message string
8DB8 A0000000    LEA EDI,DWORD PTR DS:[EAX+A0] ; Destination buffer
8BC1             MOV EAX,ECX
C1E9 02          SHR ECX,2
F3:A5            REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]
```

The *_snprintf()* function returns the total amount of bytes written, so above code would not seem to be unreasonable. The problem is that, if the source buffer is

larger than the maximum number of characters to store (*count*), a particular behavior takes place:

"If the number of bytes required to store the data exceeds count, then count bytes of data are stored in buffer and a negative value is returned" [MSDN]

Therefore, if the string is larger than 1024 bytes, after the first instruction of the presented code ECX would contain a negative number treated as unsigned, resulting in a very big number. Then, when the memory copy operation takes place, heap space reserved would be overflowed.

This will overwrite heap block structures, which would eventually be used and result in the execution of the famous set of instructions:

```
8901             MOV DWORD PTR DS:[ECX],EAX
8948 04          MOV DWORD PTR DS:[EAX+4],ECX
```

As both ECX and EAX can be controlled, an arbitrary DWORD overwrite is possible, leading to the possibility of executing arbitrary code.

Impact:

Under UNIX systems, successful exploitation of this vulnerability may allow an attacker to execute remote code with the privileges of the SAP System Administrator account (*<SID>adm)*, allowing him to take full control of the SAP system installation.

Under Microsoft Windows systems, successful exploitation of this vulnerability may allow an attacker to execute remote code with the privileges of the *LocalSystem* account, allowing him to take full control of the entire system.

Solutions:

SAP has released patches to address this vulnerability. Affected customers should apply the patches immediately.
More information can be found on SAP Note 968423.

Vendor Response:

- 2006-06-02: Initial Vendor Contact.
- 2006-06-09: Vendor Confirmed Vulnerability.
- 2006-07-03: Vendor Releases Update for version 6.40.
- 2006-07-13: Vendor Releases Update for version 7.00.
- 2006-08-10: Pre-Advisory Public Disclosure.
- 2007-01-18: Advisory Public Disclosure.

Special Thanks:

Thanks goes to Carlos Diaz and Victor Montero.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at mnunez <at> cybsec <dot> com.

For more information regarding CYBSEC: www.cybsec.com