



CYBSEC S.A.
www.cybsec.com

Pre-Advisory Name: SAP Internet Graphics Service (IGS) Undocumented Features

Vulnerability Class: Undocumented Features

Release Date: 12/05/2006

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: Medium

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 \geq 6.30)

Vulnerability Description:

Undocumented features have been discovered in SAP IGS service, some of which may signify security risks.

Technical Details:

Technical details will be released three months after publication of this pre-advisory. This was agreed upon with SAP to allow their customers to upgrade affected software prior to technical knowledge been publicly available.

Impact:

Successful exploitation of this vulnerability allows to remotely shutdown SAP IGS service, access configuration files and to perform unauthorized actions over service deployment.

Solutions:

SAP has released patches that disable the default-enabled access to the service HTTP interface. Beside, some commands has been disabled. Affected customers should apply the patches immediately.

More information can be found on SAP Notes 959358 and 965201.

Vendor Response:

- 06/02/2006: Initial Vendor Contact.
- 06/09/2006: Vendor Confirmed Vulnerability.
- 07/03/2006: Vendor Releases Update for version 6.40.
- 07/13/2006: Vendor Releases Update for version 7.00.
- 10/08/2006: Vendor Confirmed Solution.
- 12/05/2006: Pre-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.com](mailto:mnunez@cybsec.com). Please bear in mind that technical details will be disclosed to the general public three months after the release of this pre-advisory.

For more information regarding CYBSEC: www.cybsec.com