



CYBSEC S.A.

www.cybsec.com

Pre-Advisory Name: SAP Internet Graphics Service (IGS) Remote Arbitrary File Removal

Vulnerability Class: Path Traversal

Release Date: 12/05/2006

Affected Applications:

- SAP IGS 6.40 Patchlevel ≤ 16
- SAP IGS 7.00 Patchlevel ≤ 6

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 remove any file located in SAP IGS file-system.

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:

Under UNIX systems, successful exploitation of this vulnerability may allow an attacker to remotely remove files existing on the SAP IGS file-system. These files must have write permission for SAP System Administrator account (<SID>adm).

Under Microsoft Windows systems, successful exploitation of this vulnerability may allow an attacker to remove any files existing on the SAP IGS file-system.

Solutions:

SAP has released patches to address this vulnerability. Affected customers should apply the patches immediately.

Vendor Response:

- 11/03/2006: Initial Vendor Contact.
- 11/06/2006: Vendor Confirmed Vulnerability.
- 11/29/2006: Vendor Releases Update for version 6.40.
- 11/29/2006: Vendor Releases Update for version 7.00.
- 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