



CYBSEC S.A.

www.cybsec.com

Pre-Advisory Name: SAP RFC_START_GUI RFC Function Buffer Overflow

Vulnerability Class: Buffer Overflow

Release Date: 2007-04-03

Affected Applications:

- SAP RFC Library 6.40
- SAP RFC Library 7.00

Affected Platforms:

- AIX 32bit
- AIX 64bit
- 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
- Mac OS
- OS/400
- OS/400 V5R2M0
- Reliant 32bit
- Solaris on SPARC 32bit
- Solaris on SPARC 64bit
- Solaris on x64_64 64bit
- TRU64 64bit
- Windows Server on IA32 32bit
- Windows Server on IA64 64bit
- Windows Server on x64 64bit
- z/OS 32bit

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 RFC Library offers an interface to a SAP System. The RFC Library is the most commonly used and installed component of existing SAP Software. This interface provides the opportunity to call any RFC Function in a SAP System from an external application. Moreover, the RFC Library offers the possibility to write a RFC Server Program, which is accessible from any SAP System or external application. Most SAP Connectors use the RFC Library as communication platform to SAP Systems.”

RFC_START_GUI RFC Function is used to start SAPGUI on front-end systems. This function is installed by default in every external RFC server.

Vulnerability Description:

A remote buffer overflow vulnerability has been detected in the *RFC_START_GUI* RFC Function.

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:

This vulnerability may allow an attacker to remotely execute arbitrary commands over external RFC servers.

Solutions:

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

More information can be found on SAP Note 1003908.

Vendor Response:

- 2006-11-21: Initial Vendor Contact.
- 2006-12-01: Vendor Confirmed Vulnerability.
- 2006-12-11: Vendor Releases Update for version 6.40.
- 2006-12-11: Vendor Releases Update for version 7.00.
- 2007-04-03: Pre-Advisory Public Disclosure.

Special Thanks:

Thanks goes to Victor Montero and Gustavo Kunst.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at [mnunez <at> cybsec <dot> com](mailto:mnunez@cybsec.com).

About CYBSEC S.A. Security Systems

Since 1996 CYBSEC S.A. is devoted exclusively to provide professional services specialized in Computer Security. More than 150 clients around the globe validate our quality and professionalism.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.