



CYBSEC S.A.
www.cybsec.com

Advisory Name: Arbitrary File Read/Delete in SAP BC (Business Connector)

Vulnerability Class: Improper Input Validation

Release Date: 05/15/2006

Affected Applications:

- SAP BC 4.6
- SAP BC 4.7

Affected Platforms:

- Platform-Independent

Local / Remote: Remote

Severity: Medium

Author: Leandro Meiners.

Vendor Status:

- Confirmed, patch released.

Reference to Vulnerability Disclosure Policy:

http://www.cybsec.com/vulnerability_policy.pdf

Product Overview:

SAP Business Connector (SAP BC) is a middleware application based on B2B integration server from webMethods. It enables communication between SAP applications and SAP R/3 and non-SAP applications, by making all SAP functions accessible to business partners over the Internet as an XML-based service.

The SAP Business Connector uses the Internet as a communication platform and XML or HTML as the data format. It integrates non-SAP products by using an open, non-proprietary technology.

Vulnerability Description:

SAP BC was found to allow reading and deleting any file from the file system to which the user that the SAP BC is running as had access. The vulnerability is present in the Monitoring functionality of the SAP Adapter.

Technical Details:

When you view a log file (such as `new_sap.log`) the URL used is:

`https://sapbc/SAP/chopSAPLog.dsp?fullName=packages%2FSAP%2Flogs%2Fnew_sap.log`

If the `fullName` parameter is changed to `/etc/passwd` (URL encoded) instead of `<SAP PATH>/packages/SAP/logs/new_sap.log` been viewed, the contents of the file `/etc/passwd` are presented to the user. As mentioned before any file on the File System to which the user that the SAP BC is running as has read access can be viewed.

The following URL (designed to allow deletion of log files) allows deleting any file on the File System that the user the SAP BC is running as can delete.

`http://sapbc/invoke/sap.monitor.rfcTrace/deleteSingle?fullName=<path_to_file>`

Impact:

The Business Connector by default runs as a privileged user (*administrator* on the Windows platform and *root* on *NIX platforms), which allows **ANY** file on the File System to be read/deleted.

According to the SAP Business Connector Security Best Practices, the following strategies are recommended for running the SAP BC in *NIX environments:

1. Running as non root user, using a high port.
2. Running as non root user, using a high port and port remapping to "see" the SAP BC in a restricted port.
3. Running the JVM setuid root.
4. Running SAP BC as root

If either strategy (1) or (2) was taken the scope of the vulnerability was mitigated to allowing read/delete access to only the files owned by the user which the BC was running as. However, if (3) or (4) had been chosen **ANY** file on the File System could be read/deleted from the BC. Moreover, (3) allowed any user of the Operating System to obtain *root* since any Java program would be run with root privileges due to a *SetUid* Java Virtual Machine.

The SAP Business Connector Security Best Practices has been corrected to recommend running the BC as a non-root user and using a high-numbered port or, if supported by the Operating System, giving the user privileges to open a specific port below 1024 to be used by the BC.

Solutions:

SAP released a patch regarding this issue, for versions 4.6 and 4.7 of SAP BC. Details can be found in SAP note 906401.

Vendor Response:

- 12/06/2005: Initial Vendor Contact.
- 12/07/2005: Technical details for the vulnerabilities sent to vendor.
- 01/20/2006: Solution provided by vendor.
- 02/15/2006: Coordinate release of pre-advisory without technical details.
- 05/15/2006: Coordinate release of advisory with technical details.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at lmeiners@cybsec.com.

For more information regarding CYBSEC: www.cybsec.com