



**CYBSEC S.A.**  
[www.cybsec.com](http://www.cybsec.com)

**Pre-Advisory Name:** Phishing Vector in SAP BC (Business Connector)

**Vulnerability Class:** Phishing Vector / Improper Input Validation

**Release Date:** 02/15/2006

**Affected Applications:**

- SAP BC Core Fix 7 (and below)

**Affected Platforms:**

- Platform-Independent

**Local / Remote:** Remote

**Severity:** Low

**Author:** Leandro Meiners.

**Vendor Status:**

- Confirmed, patch released.

**Reference to Vulnerability Disclosure Policy:**

[http://www.cybsec.com/vulnerability\\_policy.pdf](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 provide a vector to allow Phishing scams against the SAP BC administrator.

### **Technical Details:**

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

### **Impact:**

This can be used to mount a Phishing scam by sending a link, that if clicked by the administrator (while logged in, or logs in after clicking) will load the attacker's site webpage inside an HTML frame.

### **Solutions:**

SAP released a patch regarding this issue, which requires Server Core Fix 7. Details can be found in SAP note 908349.

### **Vendor Response:**

- 12/06/2005: Initial Vendor Contact.
- 12/07/2005: Technical details for the vulnerabilities sent to vendor.
- 12/19/2005: Solutions 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 [imeiners<at>cybsec.com](mailto:imeiners@cybsec.com). Please bear in mind that technical details will be disclosed three months after the release of this pre-advisory, so such questions won't be answered until then.

For more information regarding CYBSEC: [www.cybsec.com](http://www.cybsec.com)