



CYBSEC S.A.
www.cybsec.com

Advisory Name: Phishing Vector in SAP WAS (Web Application Server)

Vulnerability Class: Phishing Vector / Improper Input Validation

Release Date: 11/09/2005

Affected Applications:

- SAP WAS 6.10
- SAP WAS 6.20
- SAP WAS 6.40
- SAP WAS 7.00

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 Web Application Server is an open standard-based platform for developing, and implementing Web applications. SAP Web Application Server is a crucial component of mySAP® Technology platform as it serves as the underlying infrastructure for many SAP solutions (for example, SAP Portal).

SAP WAS provides a development infrastructure on which to develop, distribute, and execute platform-independent Web services and business applications. SAP Web Application Server supports ABAP, Java, and Web services.

The vulnerability discovered only applies to the BSP runtime of SAP WAS.

Vulnerability Description:

SAP Web Application Server was found to provide a vector to allow Phishing scams against SAP WAS applications.

Exploit:

The parameter **sap-exiturl** allows absolute URLs, such as <http://www.google.com> by specifying "http://" as "http%3a%2f%2f". This together with the parameter **sap-sessioncmd**, can be used to mount a Phishing scam by sending a link like <http://sap-was/sap/bc/BSp/sap/menu/fameset.htm?sap-sessioncmd=close&sapexiturl=http%3a%2f%2fwww.attacker.com> that will logout the user from the application (sap-sessioncmd=close), even if not logged in, and redirect to the attacker site.

Solutions:

The solution, provided by SAP, is to disable support for the parameter in older 6.10 releases as well as SP's in 6.20 prior to SP54. For new 6.20 and 7.00 releases the **sap-exiturl** parameter will be submitted to a customer configured white-list. For further information see SAP Note 887322.

Vendor Response:

- 09/23/2005: Initial Vendor Contact.
- 09/27/2005: Technical details for the vulnerabilities sent to vendor.
- 10/14/2005: Solutions provided by vendor for all vulnerabilities.
- 11/09/2005: Coordinate release of advisory.

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