CYBSEC S.A.
www.cybsec.com

Advisory Name: Multiple XSS in SAP WAS (Web Application Server)

Vulnerability Class: Cross-Site Scripting

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 be vulnerable to JavaScript injection, allowing for Cross-Site Scripting attacks. Three different vectors for script injection where discovered:

- Error Pages (in error messages displayed) (SAP WAS 6.20 and above **not** Vulnerable)
- The **syscmd** parameter
- SYSTEM PUBLIC (Test Application)

Exploit:

Following is a Proof of Concept for each script injection vector:

- Error Pages:

http://sap-was/sap/bc/BSp/sap/index.html%3Cscript%3Ealert('xss')%3C/script%3E

- The **syscmd** parameter:

http://sap-was/sap/bc/BSp/sap/menu/frameset.htm?sap-sessioncmd=open&sap-syscmd=%3Cscript%3Ealert('xss')%3C/script%3E

- Test Application (SYSTEM PUBLIC):

In BspApplication field it is possible to inject JavaScript code such as: “<script>alert(‘xss’)</script>.

Solutions:

For solutions regarding Error Pages and the **syscmd** parameter as attack vectors please see SAP Note 887323, which indicates Service Packs to apply.

For solutions regarding SYSTEM PUBLIC Test Application please see SAP Note 887164 which lists all test applications that **shouldn’t** be activated on production systems. Regarding XSS issues the BSP compiler has been extended to have a new forceEncode=”HTML” page directive, for more information see SAP Note 887168. This new feature will be applied to test applications in the next SP cycle. **All** test applications should always be removed from production systems, customers can use transaction SMICM to disable the test applications.

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.

Thanks:

Special thanks go to Mariano Nuñez Di Croce.

Contact Information:

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

For more information regarding CYBSEC: www.cybsec.com