



CYBSEC S.A.
www.cybsec.com

Pre-Advisory Name: Local Privilege Escalation in SAP sapdba Command

Vulnerability Class: Insecure Environment Variable Handling

Release Date: 05/18/2006

Affected Applications:

- sapdba command for Informix version prior to 700
- sapdba command for Informix version 700 up to patch number 100

Unaffected Applications:

- sapdba command for Oracle Databases

Affected Platforms:

- SAP with Informix on HP-UX, Solaris, AIX, TRUE64 or Linux

Local / Remote: Local

Severity: Medium

Author: Leandro Meiners.

Vendor Status:

- Confirmed, patch released

Reference to Vulnerability Disclosure Policy:

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

Product Overview:

The **sapdba** command is a utility provided by SAP for database administration. Two different versions are available, one for Informix and another for Oracle databases.

Vulnerability Description:

The **sapdba** command for Informix Databases was found to allow any UNIX user to run arbitrary commands with *informix* rights at the shell level, due to improper handling of environment variables.

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:

Any user with login access to the SAP database server having a vulnerable version of the **sapdba** command can escalate privileges to execute arbitrary commands with the rights of the *informix* user.

Solutions:

SAP released a patch regarding this issue. Details can be found in SAP note 944585.

Vendor Response:

- 04/20/2006: Initial Vendor Contact and technical details for the vulnerabilities sent to vendor.
- 04/26/2006: Solution provided by vendor.
- 05/18/2006: Coordinate release of pre-advisory without technical details.
- 08/18/2006: 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