Technical Bulletin – Issue #2

© February 2003 Soft Design A/S

This Technical Bulletin contains important information and recommendations regarding the security of applications developed with Websydian.

WEBSYDIAN SECURITY UPDATE

In Websydian the cryptographic hashing algorithm MD2 is used for password verification in Websydian's User Management pattern and for providing manipulation detection codes in the Integrity Control pattern, both part of Websydian Web Developer. It has been discovered that the Websydian MD2 implementation is incorrect.

Analysis has found the implemented algorithm to be weaker than proper MD2. However, further analysis performed by cryptographic experts has shown that the uncovered vulnerability will not affect security in Websydian's standard patterns, or applications, which use these patterns in a standard fashion.

UPDATE CONSIDERATIONS

An update to a proper MD2 implementation in Websydian is now available. Information on how to install this update can be found in the "Upgrade Guide for MD2 Update". Updates and guides are included in the Websydian v4.0 release and are available for Websydian v2.0 and up.

Upgrading existing applications to proper MD2 affects all passwords stored using Websydian's User Management pattern. To avoid blocking access to existing users, refer to the guide "Update Passwords in User Management Pattern" for directions on how to migrate stored passwords for existing users.

RECOMMENDATIONS

- **For standard uses in Websydian's User Management and Integrity Control patterns**
  Soft Design assesses the deviating algorithm to provide a comparable level of security to proper MD2 for standard Websydian password verification and integrity control. However, as a precautionary measure, we recommend Websydian applications be moved to the proper MD2 implementation as part of the next planned application upgrade.

- **For other uses of MD2**
  Since the incorrect MD2 implementation is weaker than proper MD2 for general use, Soft Design recommends that Websydian applications be reviewed for non-standard uses of MD2 and, if needed, changed to use of MD2 proper as soon as possible.

  Note that if Websydian-generated MD2 values are used with 3rd party software, it is necessary to use the proper MD2 algorithm for compatibility.