



CYBSEC S.A.
www.cybsec.com

Advisory Name: Default Configuration Information Disclosure in Lotus Domino
(Including password hashes)

Vulnerability Class: Default Configuration/Information Disclosure

Release Date: 07/26/2005

Affected Applications:

- Lotus Domino R5 WebMail
- Lotus Domino R6 WebMail
- Lotus Domino R4 wasn't audited.

Affected Platforms:

- Platform-Independent

Local / Remote: Remote

Severity: High

Author: Leandro Meiners.

Vendor Status:

- Configuration fix supplied by vendor.

Reference to Vulnerability Disclosure Policy:

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

Overview:

IBM Lotus Domino is an integrated collaborative environment, which allows messaging, calendaring and scheduling capabilities. IBM Lotus Domino WebMail is one of the client components for accessing Lotus Domino messaging capabilities, which provides a Web interface to Lotus Domino.

Vulnerability Description:

The main directory database for Lotus Domino, names.nsf, defined as the Public Address Book is by default readable by all users. Therefore, all users are allowed to view a person's entry.

When any unprivileged user views a person's entry there is a field called "Internet Password" that is blank, meaning that the user can't view the password hash. However, if the Web page is edited ("view page source" in Internet Explorer) there is a hidden field called "HTTPPassword" which contains the password hash.

The same problem applies to all other fields that appear as blank; if they have a value defined then that value is stored in a hidden field.

Other critical information can be retrieved (under Release 6), such as:

- The change date of the password (field "HTTPPasswordChangeDate")
- The client's platform (field "ClntPltfrm")
- The client's machine name (field "ClntMachine")
- The client's Lotus Domino release (field "ClntBld")

Exploit:

No exploit required. Nevertheless, it is appropriate to mention that there are Lotus Domino password crackers such as Domino Hash Breaker (tested on Lotus Domino R5 and R6 with the appropriate DLL), available at <http://www.securiteinfo.com/outils/DominoHashBreaker.shtml>.

Furthermore, the algorithm used by Lotus Domino to hash the password doesn't use a salt, meaning that the string "355E98E7C7B59BD810ED845AD0FD2FC4" is always the hash for the string "password". This allows passwords to be pre-computed in order to construct a hash database of common passwords or even all six to eight digit character combinations, minimizing the time needed to crack a password.

Solutions:

IBM's solution to the problem:

To hide the HTTP password from the HTML source:

- 1) Open the \$PersonInheritableSchema subform (In the designer under Shared Code, Subforms).
- 2) Find the fields: \$dspHTTPPassword and HTTPPassword.
- 3) In the field properties for both fields, on the hide tab under "Hide paragraph from" check off "Web browsers".
- 4) Open the Person form (Under Forms).
- 5) In the form properties, on the 2nd tab, disable the option "Generate HTML for all fields".

We found step five to be sufficient to hide all the above mentioned fields.

Vendor Response:

- 04/22/2005: Initial Vendor Contact
- 05/09/2005: Vendor response stating that they couldn't find a way to remove the hidden fields.
- 06/02/2005: Vendor opens a new case regarding the vulnerability.
- 06/28/2005: Vendor response with a configuration to fix the vulnerability.

Thanks:

Special thanks goes to Claudia Iaconis, Adrian Saucedo and Tadeo Cwierz.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at [Imeiners<at>cybsec.com](mailto:Imeiners@cybsec.com).

For more information regarding CYBSEC: www.cybsec.com