

[NEWS] Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/14/05

To: list@securiteam.com

Date: 14 Aug 2005 18:06:24 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)

SUMMARY

Lotus Domino's default settings allow unprivileged users to retrieve the product's users' hashed passwords. This hashed password can then be brute forced to recover its plaintext equivalent.

DETAILS

Vulnerable Systems:

- * Lotus Domino R5 WebMail
- * Lotus Domino R6 WebMail

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 "HTTTPassword" which contains the password hash.

[NEWS] Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)

Securiteam: [NEWS] Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)

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 \$PersonalInheritableSchema 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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:lmeiners@cybsec.com> Leandro Meiners.

Securiteam: [NEWS] Default Configuration Information Disclosure in Lotus Domino (Including Password Hashes)

The original article can be found at:

<http://www.cybsec.com/vuln/default_configuration_information_disclosure_lotus_domino.pdf>

http://www.cybsec.com/vuln/default_configuration_information_disclosure_lotus_domino.pdf

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.