

Weakness in Lotus Domino simplifies Account Theft

July 1, 2004

InfoScreen, Inc. has identified a previously unknown vulnerability in Lotus Domino systems. A common setting makes it simple to force web authentication without knowing usernames. InfoScreen recommends updating Domino servers to prevent unauthorized access.

Systems affected:

Lotus Domino servers.

Versions affected:

All versions.

Brute-force attacks of password-protected computer systems typically attempt multiple passwords against a known account. New information about the behavior of Lotus Domino servers turns this paradigm on its head. It is more practical to check most or all accounts against a small number of passwords. No knowledge of valid account names is required.

Lotus Domino, starting with R5, offers administrators a choice of two web authentication settings. The difference between these is the number of user name variations accepted by the directory lookup mechanism. The less restrictive setting is the default behavior on all Domino servers before R6. A Domino server configured to permit this "more name variations" setting is vulnerable to a novel and efficient form of account theft.

The less restrictive setting allows the input for user name to be a code called a Soundex number. The Soundex number is a short, non-unique key derived from the user name. An example is S530, equivalent to Sand, Smith, Smith99, Sunday, and many other names. It is common for a Domino directory to have multiple users associated with the same Soundex number.

If using the "more name variations" setting, User Smith may login as 'Smith' or 'S530', supplying the correct account password, and begin an authenticated session. This is most generally true of HTTP authentication. Domino handles Soundex in an inconsistent manner. Some protocols, such as IMAP, will not permit a Soundex number during authentication if the Soundex number "username" is not unique in the name and address book. HTTP and HTTPS authentication proceeds even when there are multiple matching username entries. Domino looks at each account that has the given Soundex number until finding a matching password.



There are several properties of Soundex numbers that make them a weak element in authentication. They are less variable than the names from which they are derived and offer a smaller target for attack. The distribution of Soundex numbers in a population is based on both the frequency of names and the number of names that have the same Soundex code.

The set of Soundex numbers is finite and much smaller than the set of possible usernames. At most 6734 Soundex numbers are derived from the nearly limitless set of possible usernames. This small number makes it practical to try every account name for a given password.

The distribution of Soundex numbers is less random than surnames. While the U.S. Census estimates that 1 person in 100 is named Smith, 1 in 90 has a Soundex number of S530, because Soundex number S530 matches dozens of names in addition to Smith. The 100 most common surnames account for about 1 person in 5. The 100 most common Soundex numbers match nearly 1 in 3.

These figures point to an elevated risk of forced authentication under the following circumstances:

- ◆ Domino server web authentication settings permit more name variations.
- ◆ User accounts exist with common or guessable passwords.
- ◆ Organizations that have many entries in the directory used for lookup are at particular risk.

An attempt to brute-force accounts with weak passwords is improved with Soundex information in two ways.

- ◆ To check all accounts for a common password with 100% certainty requires 6734 tries using Soundex numbers. Without Soundex this is a practical impossibility.
- ◆ To check a large proportion of accounts against a list of common passwords. Testing the top 33% of names and 20 common passwords requires 2000 tries with Soundex. This is at least four times more efficient than guessing user surnames.

Soundex numbers as usernames encourage credential theft. Even when no valid user names are known, the predictability of Soundex numbers can be used to try a given password on every possible account. Accounts with that password will be found and compromised in fewer than 10 minutes, on average. Faster results are possible by eliminating improbable Soundex numbers.



Guessing usernames with Soundex is 1000% more efficient than using last names alone. Soundex can match to the top 75% of usernames - 15000 names - with only 1300 Soundex numbers.

All R4 Domino servers behave in the less secure manner. All R5 Domino servers have the less secure behavior as the default setting. The default behavior for R6 is reversed, but many R6 users will upgrade and preserve R5-derived settings.

InfoScreen provided IBM with a statement of our findings in March 2004. IBM has provided information on the vulnerability by publishing a Technote on the subject:

<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21165495>

For additional information please contact Richard Sheiman at InfoScreen (1-800-613-1925 or sheiman@infoscreen.com).