

Full-Disclosure: RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-09/0923.html>

From: Ferris, Robin (*R.Ferris_at_napier.ac.uk*)

Date: 09/17/03

To: full-disclosure@netsys.com

Date: Wed, 17 Sep 2003 09:21:18 +0100

Damn Right, you sound like a script kiddie of the worst kind.

If you are still trying to get this working make sure you do it on a PC that isnt connected to any live network other than a test one. Whilst you are learning and I hope you are for the right reasons, make sure you dont screw it up and send something out live, like that fat bastard did with the last M\$ sploit.

Just a little flame and some words of wisdom.

RF

-----Original Message-----

From: Brown, Rodrick [mailto:rbrown@doitt.nyc.gov]

Sent: 17 September 2003 05:48

To: Elvar; SPAM; full-disclosure@netsys.com

Subject: RE: [Full-Disclosure] which DCOM exploit code are they speaking about here?

The code compiles with 0 warnings and errors here, if you really have no clue how the code works or able to fix your bad cut/paste maybe you just shouldnt be using it.

- RB

- NYC.GOV

From: full-disclosure-admin@lists.netsys.com on behalf of Elvar

Sent: Wed 9/17/2003 12:16 AM

To: 'SPAM'; full-disclosure@netsys.com

Subject: RE: [Full-Disclosure] which DCOM exploit code are they speaking about here?

I realize it's probably just my lack of skills, but this doesn't seem to

RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

Full-Disclosure: RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

compile unmodified. I do not know any C / CPP so I can't figure out what to fix to make it compile if it does indeed need modification.

Elvar

-lick your wounds

-----Original Message-----

From: full-disclosure-admin@lists.netsys.com
[mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of SPAM
Sent: Tuesday, September 16, 2003 10:09 PM
To: full-disclosure@netsys.com
Subject: Fw: [Full-Disclosure] which DCOM exploit code are they speaking about here?

I think this would be the one...

<http://packetstormsecurity.nl/0309-exploits/09.16.MS03-039-exp.c>

Ed

----- Original Message -----

From: "Josh Karp" <jkarp@visionael.com>
To: <full-disclosure@lists.netsys.com>
Sent: Wednesday, September 17, 2003 7:19 AM
Subject: [Full-Disclosure] which DCOM exploit code are they speaking about here?

>

<http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2003/09/16/nati>

> [onal1842EDT0790.DTL](#)

>

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2003/09/16/nati>

> [ional1842EDT0790.DTL](#)>

>

> *Security researchers on Tuesday detected hackers distributing software to*
> *break into computers using flaws announced last week in some versions of*
> *Microsoft Corp.'s Windows operating system.*
> *The threat from this new vulnerability -- which already has drawn stern*
> *warnings from the Homeland Security Department -- is remarkably similar to*
> *one that allowed the Blaster virus to infect hundreds of thousands of*
> *computers last month.*
> *The discovery gives fresh impetus for tens of millions of Windows users --*
> *inside corporations and in their homes -- to immediately apply a free*
> *repairing patch from Microsoft. Homeland Security officials have warned*
> *that*
> *attacks could result in a "significant impact" on the operation of the*
> *Internet.*
> *Researchers from iDefense Inc. of Reston, Va., who found the new attack*
> *software being distributed from a Chinese Web site, said it was already*
> *being used to break into vulnerable computers and implant eavesdropping*

RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

Full-Disclosure: RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

- > *programs. They said they expect widespread attacks similar to the Blaster*
- > *infection within days.*
- > *"It's fairly likely," said Ken Dunham, a senior iDefense analyst.*
- "Certainly
- > *we'll see new variants in the next few hours or days."*
- > *Microsoft confirmed it was studying the new attack tool.*
- > *Last month's Blaster infection spread just days after hackers began*
- > *distributing tools for breaking into Windows computers using a related*
- > *software flaw. That infection disrupted computers at the Federal Reserve*
- in
- > *Atlanta, Maryland's motor vehicle agency and the Minnesota transportation*
- > *department.*
- > *The latest Windows flaws, announced Sept. 10, were nearly identical to*
- those
- > *exploited by the Blaster worm. Computer users who applied an earlier patch*
- > *in July to protect themselves still must install the new patch from*
- > *Microsoft, available from its Web site.*
- > *Amy Carroll, a director in Microsoft's security business unit, said 63*
- > *percent more people have already downloaded the latest patch than*
- downloaded
- > *the patch for last month's similar vulnerability during the same five-day*
- > *period.*
- > *"We've continued to beat the drum, to give people better awareness,"*
- Carroll
- > *said. "We have seen some success."*
- > *The latest hacker tool was relatively polished. It gives hackers access to*
- > *victims' computers by creating a new account with the name "e" with a*
- preset
- > *password. iDefense said the tool includes options to attack two Windows*
- 2000
- > *versions that are commonly used inside corporations.*
- > *The tool being distributed Tuesday did not include an option to break into*
- > *computers running Microsoft's latest operating systems, such as Windows XP*
- > *or Windows Server 2003, but iDefense said it expected such modifications*
- to
- > *make it more dangerous.*
- >
- > *On the Net:*
- > *Microsoft warning:*
- > *www.microsoft.com/security/security_bulletins/ms03-039.asp*
- > *<http://www.microsoft.com/security/security_bulletins/ms03-039.asp>*
- > *Homeland Security warning:*
- > *www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm*
- > *<<http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm>>*
- >
- >
- >
- >

Full-Disclosure – We believe in it.

RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

Full-Disclosure: RE: [Full-Disclosure] which DCOM exploit code are they speaking a bout here?

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>