

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

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

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-09/0946.html>

From: James Foster (*James.Foster_at_foundstone.com*)

Date: 09/17/03

To: "Brown, Rodrick" <rbrown@doitt.nyc.gov>, "Elvar" <elvar@ooz.net>, <full-disclosure@netsys.com>

Date: Tue, 16 Sep 2003 22:34:26 -0700

If you are trying to compile within Visual Studio then the compile-time conversion errors can be alleviated with a "(char *)" in front of the second parameter

-Foster

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 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>

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

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

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/nat>

> *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*

> *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.*

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

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

- > *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>>*
- >
- >
- >
- >

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

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

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>

Full-Disclosure – We believe in it.

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