

MS01-058 exploit - W32/Cool.A-mm

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-12/0024.html>

From: Steen Larsen (slarsen@MESSAGELABS.COM)

Date: 12/18/01

Date: Tue, 18 Dec 2001 16:16:49 -0000
From: Steen Larsen <slarsen@MESSAGELABS.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

There is apparently an email circulating with a link to a site that exploits the MS01-058 vulnerability.

The text is the following:

Hi. I found cool site! <http://celebxx.cjb.net> It's really cool!

The subject is: Hi!!

Please note that this is early information that has not been properly researched yet.

Best regards

Steen Larsen

More information will be available on:

<http://www.messagelabs.com/viruseye/threatlist.asp>

See W32/Cool.A-mm

Steen Larsen
Director of Security
MessageLabs Ltd.

E - slarsen@messagelabs.com

DD - +44 (0) 1452 627639

F - +44 (0) 1452 627628

W - www.messagelabs.com

Company Registration No - 834506

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

From: Russ [mailto:Russ.Cooper@RC.ON.CA]

NT-Bugtraq: MS01-058 exploit - W32/Cool.A-mm

Sent: 18 December 2001 15:27

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Subject: Re: MS01-058 broke my IE6

A number of people have contacted me about the lack of any message regarding the availability of MS01-058.

Microsoft issued the patch on December 13th, 2001, and on the 14th I received two messages (below) indicating it (the patch) had broken the system it was installed on. I contacted the Microsoft Security Response Center and they indicated they hadn't received any other reports of problems (as of the 14th) and hadn't heard of customers reporting problems deploying it.

I thought to wait for more feedback (two reports of problems really isn't enough to go out with a warning on), or for MS to remove the patch (if they got enough reports). I was also aware of the *potential* for MS to release v2.0 to address the issues that HTTP-Equiv rose.

So I've held off mentioning the patch;

<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>

But then you have the dire warnings coming from some media outlets that IE users need to patch Now!

Firstly, of the few IE vulnerabilities that we have actually seen exploited (or attempted) en-masse, they have typically come several months after the release of exploit code. Also, when they're dependent on a server being up to deliver the payload, they don't spread far (or the part that works with the payload stops working because the site has been taken down).

This isn't to say the patch doesn't address serious issues, Microsoft's Severity Rating for systems running IE 6.0 is "Critical" across the board.

However, the urgency with which you need to deploy this is offset by the potential for problems deploying. I'd choose to err on the side of caution given the installation reports below, and make sure you install on a system

NT-Bugtraq: MS01-058 exploit – W32/Cool.A-mm

you don't mind destroying before you deploy across your organization.

If anyone else has experienced problems with MS01-058, let me know.

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

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

From: Jeff Lether

Sent: Friday, December 14, 2001 11:32 AM

To: Russ.Cooper@rc.on.ca

Subject: MS01-058 broke my IE6

I am running Win2K w/ SP2, fully patched in all respects (according to both MSPSA, HFNetChk, and Windows Update). This morning, like everyone else I received the dire warnings contained in MS security bulletin MS01-058 and installed the patch immediately, as urged by Microsoft.

Now, after rebooting (several times!) I can no longer use IE 6.0 (or any program which depends on it). IE will launch normally, and you can view the about window to see that the patch was installed. But the second you try to navigate to any web site (doesn't matter which, I've tried several), IE locks up and stops responding to anything. It will not respond to the task manager trying to close it, insisting instead that it is being debugged, and to close the debugger first. You also cannot shut down windows normally either. The shutdown sequence just hangs when trying to forcibly close the non-responding IE. You wind up having to actually power off your system to get IE out of memory.

Jeff Lether

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

From: David C. Dunthorn

Sent: Fri, 14 Dec 2001 11:24:22 -0500

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Subject: MS01-058 broken?

NTBugtraq members,

When I installed the MS-01-058 cumulative patch for IE6 and my machine rebooted, It locked up when changing display modes. I tried rebooting in

vga mode and then changing display modes to one I know works the screen again went blank and the machine locked. Even when I booted to vga mode and selected the current display mode and pressed the test button it didn't work. What _did_ work was pressing the cancel button to not change the display mode and then reinstall sp6. When the machine rebooted I let it come up in my normal display mode and everything worked fine. All I've had to do since then is reinstall any post sp6 updates that I needed. I hope that this is just happening to me, but when I tried to get to the NTBugtraq web site I got no response, so I thought this message might be in order.

David C. Dunthorn

=====
=====
Delivery co-sponsored by VeriSign - The Internet Trust Company
=====
=====
Protect your servers with 128-bit SSL encryption!
Get VeriSign's FREE guide, "Securing Your Web Site for Business." You will learn everything you need to know about using SSL to encrypt your e-commerce transactions for serious online security. Click here!
<http://www.verisign.com/cgi-bin/go.cgi?a=n016065650057000>
=====
=====

This email has been scanned for all viruses by the MessageLabs SkyScan service.
For more information on a higher level of virus protection visit www.messagelabs.com

This email has been scanned for all viruses by the MessageLabs SkyScan service.
For more information on a higher level of virus protection visit www.messagelabs.com

-
- **Previous message:** [Russ: "Re: MS01-058 broke my IE6"](#)
 - **Next in thread:** [Russ: "Re: MS01-058 exploit - W32/Cool.A-mm"](#)
 - **Reply:** [Russ: "Re: MS01-058 exploit - W32/Cool.A-mm"](#)
 - **Reply:** [Steen Larsen: "Re: MS01-058 exploit - W32/Cool.A-mm"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)