

Re: Microsoft's GDI Detection Tool faults

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-09/0379.html>

From: Andreas Marx (amarx_at_gega-it.de)

Date: 09/26/04

Date: Sun, 26 Sep 2004 18:38:18 +0200

To: Gadi Evron <ge@linuxbox.org>, John Bissell <monkey321_1@hotmail.com>

Hello!

>*I have some things to say to you, and others. Then I will elaborate on
>_yet_another_JPEG vulnerability.*

Yes, it's true that there is another JPEG vulnerability. Anyway, it looks like a crash bug only (nul pointer reference) which is not exploitable. There are many ways to crash IE using this problem (with malformed JPEGs). Microsoft (secure@microsoft.com) is aware of this issue for some months and according to them, it will be fixed with the next Windows Service Packs (yes, this means Windows 2000 SP5 and Windows XP SP3).

>*I'll reply in the following order: 4. *New* JPEG vulnerability. (Let's
>hype it!)*

No, do not hype it!

>*Unlike that vulnerability, this one works on SP2 but doesn't seem to be
>exploitable.*

Exactly. It is "only" a crash bug -- and many more of these crash bugs exist in Windows and other operating systems. No need for any kind of hype.

BTW: The current status of AV detection of the MS04-028 issue is (sorted after product names; including name and status changes, all times in GMT in the format DD.MM.YYYY HH:MM):

- Antivir 23.09.2004 17:51 "TR/Exploit.MS04-28 (exact)"
- Bitdefender 24.09.2004 14:21 "Exploit.Win32.MS04-028.Gen"
- Dr. Web 21.09.2004 10:51 "Exploit.MS04-028"
- eTrust (CA Engine) 22.09.2004 22:23 "JPEG.MS04-028.Exploit.Trojan"
- eTrust (VET Engine) 23.09.2004 06:38 partly detected as "JPEG.MS04-028.exploit"
- eTrust (VET Engine) 24.09.2004 06:40 fully detected as "JPEG.MS04-028.exploit"
- F-Secure 20.09.2004 08:46 "Exploit.Win32.MS04-028.gen"
- Kaspersky 23.09.2004 12:56 "Exploit.Win32.MS04-028.gen"

SecurityFocus Bugtraq: Re: Microsoft's GDI Detetection Tool faults

- McAfee 16.09.2004 23:20 "Exploit-MS04-028" and "Exploit-MS04-028.demo"
- Panda 24.09.2004 13:30 partly detected as "Exploit/MS04-028"
- Symantec 16.09.2004 03:38 partly detected as "Bloodhound.Exploit.13"
- Symantec 18.09.2004 03:42 fully detected as "Bloodhound.Exploit.13" and "Download.Trojan"
- Trend Micro 18.09.2004 06:10 "Exploit-MS04-028"

For this list, we have tested 29 different products. "Partly detected" means that only some files out of our testbed are detected right now, but not all, like some self-generated JPEGs with this exploit. Last update: Sunday, 26.09.2004, 12:00 h GMT.

More information about this bug, the new JPEG problem, an exploit generator etc. can be found here in German language:

<<http://www.heise.de/newsticker/meldung/51459>>

cheers,
Andreas Marx
CEO, AV-Test.org

--

AV-Test GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone: +49 (0)391 6075466, <<http://www.av-test.org>>