

Re: MS04-027 and MS04-028 not detected

Source: <http://www.tech-archive.net/Archive/SMS/microsoft.public.sms.tools/2004-09/0027.html>

From: Stefan Kanthak (*postmaster_at_1.0.0.127.in-addr.arpa*)

Date: 09/16/04

Date: Thu, 16 Sep 2004 12:03:18 +0200

"Doug Neal [MSFT]" <dugn@online.microsoft.com> wrote:

Fup2 microsoft.public.security.baseline_analyzer set!

[MBSA can't detect everything]

- > *As a company, we created the GDI+ Detection tool (available for download and*
- > *through Windows Update) to help centralize the detection effort across*
- > *products MBSA doesn't support (see the full list at KB306460).*
- >
- > *It's true that MBSA will not be able to detect the patch status except for*
- > *local scans of Microsoft Office products (6 of the 26 potential affected*
- > *platforms/products), but we're directing users to the GDI+ Detection tool as*
- > *a method to identify all cases*

Are you sure?

The GDI+ detection tool does NOT detect Visio Viewer, a Microsoft "product".
It also doesn't detect third party software which redistributes GDIPLUS.DLL.

- > *and apply the appropriate patch separate from*
- > *the limited guidance MBSA can provide in this case. The additional*
- > *technical information in the MSRC bulletin (MS04-028) provides enough detail*
- > *for the technically minded to create other solutions/use other methods that*
- > *may be more appropriate for their environment to identify and patch all*
- > *cases of the vulnerable GDI+ instances.*

The security bulletin and the MSKB articles don't even mention Visio Viewer
(I suspect there may be more MSFT products missing) nor give a hint that
third party products incorporating GDIPLUS.DLL should be checked too!

- > *With a good understanding of the security requirements of our customers*
- > *we're working to ensure even better vulnerability assessment in the future.*

I still don't see that "trustworthy computing" MSFT has announced comes real!

- > *I hope that helps...*

Not yet, not completely!
Stefan

> *Doug Neal [MSFT]*
> *dugn@online.microsoft.com*
>
> *This posting is provided "AS IS" with no warranties, and confers no rights.*
>
> *If newsgroup discussion with experts and MVPs is unable to solve a problem*
> *to your satisfaction, feel free to contact PSS for the Microsoft Baseline*
> *Security Analyzer (MBSA) at the following link:*
> *<http://support.microsoft.com/default.aspx?scid=fh;en-us:Prodoffer20a>*
>
> *This e-mail address does not receive e-mail, but is used for newsgroup*
> *postings only.*
>
>
> *"Gerry Hickman" <gerry666uk@yahoo.co.uk> wrote in message*
> *news:epQeyr1mEHA.3396@tk2msftngp13.phx.gbl...*
>> *Hi Doug,*
>>
>>> *MBSA does not support either of these patches for patch detection,*
>>
>> *I have to say I find this REALLY disappointing. The whole point of a tool*
>> *like MBSA is to be able to check file versions against installed products,*
>> *NOT just say to people "you may need a patch, but we don't really know".*
>>
>> *This "note" message is no more use than going to the Microsoft security*
>> *site. It does not tell you if a machine needs patched or not. What if you*
>> *have reinstall one of the many vulnerable products – the tool won't tell*
>> *you you're open to attack again...*
>>
>> *It's also disappointing that this newer release 1.2.1 still cannot test*
>> *missing Microsoft Office patches, unless you install it on 1000+ machines*
>> *and run it locally? Conversely Shavlik's product does this without any*
>> *problem.*
>>
>> *I realise MBSA is free, but it's supposed to be part of Microsoft's drive*
>> *towards secure computing, and these limitations relate to thier OWN*
>> *flagship products (Windows and Office)!*
>>
>> --
>> *Gerry Hickman (London UK)*