

Forum: [Hack Forums](#)

Thread: [Flash Player vulnerability exploited](#)

-Hyperion - January 21, 2015, 5:24 pm

It's probably smart to disable or remove your Flash player for at least the next few days. Malware don't need coffee discovered an unpatched vulnerability (zero day attack) in Flash Player today that is being exploited by an attack tool called the Angler Exploit Kit. This attack could potentially harm many computers because it targets everyone who visits a website that contains malicious code and who's security software doesn't block the malware. - See more at:

<http://blog.emsisoft.com/2015/01/22/zero-day-alert-flash-player-vulnerability-exploited/#sthash.5xAU2DfR.dpuf>

Update MBAE does block it

<https://blog.malwarebytes.org/exploits-2/2015/01/new-adobe-flash-zero-day-found-in-the-wild/>

Kingstonz - January 21, 2015, 5:26 pm

Thanks for the heads up, i will disable flash on my parallels desktop!

Not trying to be cocky but i love my mac.

Sorry if you disagree with me.

NoScript - January 21, 2015, 5:42 pm

Thanks for the warning, Disabled with <3

Ghanem - January 21, 2015, 5:45 pm

sighs

This is why people hope MBAE would help.

Thanks for the share, hope this is fixed soon.

-Hyperion - January 21, 2015, 7:21 pm

(Jan 21, 2015 06:45 PM)Ghanem Wrote: [\[CITE\]](#) *sighs*

This is why people hope MBAE would help.

Thanks for the share, hope this is fixed soon.

MBAE will not work against a 0 day until it patched

Null Byte - January 21, 2015, 8:33 pm

(Jan 21, 2015 06:45 PM)Ghanem Wrote: [\[CITE\]](#) *sighs*

This is why people hope MBAE would help.

Thanks for the share, hope this is fixed soon.

MBAE stops these types of attacks with pretty impressive accuracy.

Null Byte - January 21, 2015, 10:03 pm

(Jan 21, 2015 09:39 PM)Yani Wrote: [\[CITE\]](#) Actually it does. It doesn't only check for signatures but also checks if something got executed trough the guarded processes, like cmd.exe for example. So this could in fact stop 0 days.

It still depends on how the exploit works though, as it can use different methods.

This. MBAE is designed to stop zero-days and uses heuristics and virtualization of browser plugins,

as well as the browser itself. Rest assured exploits such as these won't stand a chance making it through.

Ahri????? - January 21, 2015, 10:08 pm

I was about to go remove my flash until I noticed I don't even have flash, HTML 5 has replaced my need for flash.

Ghanem - January 22, 2015, 1:32 am

(Jan 21, 2015 09:39 PM)Yani Wrote: [\[CITE\]](#) It doesn't only check for signatures

As far as I understood, it doesn't check for signatures at all.

Hence it's so small, it does exactly what you said and check a program's behavior.

But still, none of you has a flash 0Day to test MBAE out I guess.

So nobody knows if it'd actually work.

Play Boy - January 22, 2015, 1:39 am

Thanks for the heads up. ?

I will be disabling flash for awhile.

-Hyperion - January 22, 2015, 3:29 am

Now it is actually tested I can say that it does block it

<https://blog.malwarebytes.org/exploits-2/2015/01/new-adobe-flash-zero-day-found-in-the-wild/>

before it is hit or miss with a 0 day.

Ghanem - January 22, 2015, 4:12 am

Hail MBAE then.

This is one of the best protection software I met.