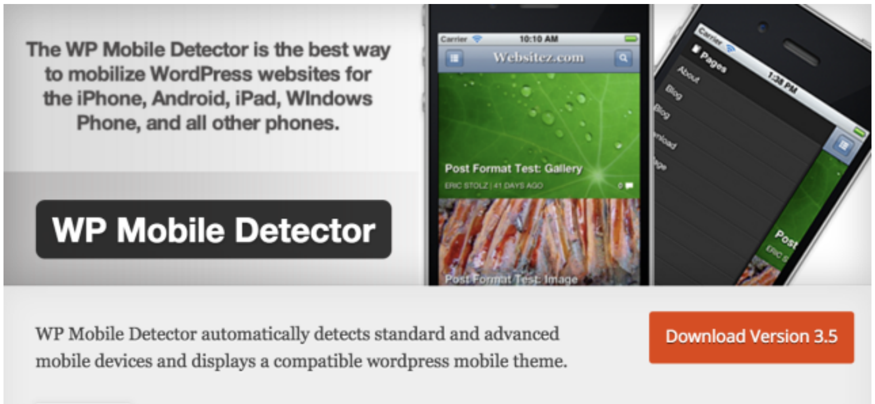
RISK ASSESSMENT / SECURITY & HACKTIVISM

WordPress plugin with 10,000+ installations being exploited in the wild

No fix available for critical flaw that's been under attack since last week.

by **Dan Goodin** - Jun 2, 2016 12:47pm PDT

27



The WP Mobile Detector is the best way to mobilize WordPress websites for the iPhone, Android, iPad, WIndows Phone, and all other phones.

WP Mobile Detector

WP Mobile Detector automatically detects standard and advanced mobile devices and displays a compatible wordpress mobile theme.

Download Version 3.5

Enlarge

A growing number of WordPress websites have been infected by attackers exploiting a vulnerability that remains unpatched in a widely used plugin called WP Mobile Detector, security researchers warned.

The attacks have been under way since last Friday and are mainly being used to install porn-related spamming scripts, according to a blog post published Thursday. The underlying vulnerability in WP Mobile Detector came to light on Tuesday in this post. The plugin has since been removed from the official WordPress plugin directory. As of Wednesday, the plugin reportedly had more than 10,000 active installations, and it appears many remained active at the time this post was being prepared.

The security flaw stems from the plugin's failure to remove malicious input submitted by website visitors. Because the WP Mobile Detector performs no security checks, an attacker can feed malicious PHP code into requests received by websites that use the plugin.

"The vulnerability is very easy to exploit," Sucuri security analyst Douglas Santos wrote. "All the attacker needs to do is send a request to resize.php or timthumb.php (yes, timthumb, in this case it just includes resize.php), inside the plugin directory with the backdoor URL."

Uninstall now

With no update available, the most sensible course of action for vulnerable websites is to completely uninstall WP Mobile Detector. A partial fix involves disabling PHP execution in the plugin's subdirectory, but that measure doesn't stop attackers from uploading malicious files to that directory and linking to them elsewhere online. Website administrators may also revoke write permissions altogether in the subdirectory, but that may prevent the plugin from working. Most application level firewalls don't provide meaningful protection against the exploits either, although Sucuri said its firewall service does provide a patch using a virtual hardening engine. The vulnerability can be exploited only when PHP option allow_url_fopen is enabled.

If the exploit's invocation of resize.php sounds familiar, it may be because of the recent vulnerability detected in ImageMagick, a widely used image-processing library that many sites use directly or indirectly to resize images uploaded by end users. However, Sucuri CTO Daniel Cid told Ars that

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Nvidia GTX 1070 review: Faster than the Titan, at a more reasonable price

Not quite the bargain the 970 was, but the GTX 1070 remains the card to beat.

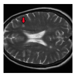
WATCH ARS VIDEO

Sunspring | A Sci-Fi Short Film Starring Thomas Middleditch

For *Sunspring*'s exclusive debut on Ars, we talked to the filmmakers about collaborating with an AI.

STAY IN THE KNOW WITH

LATEST NEWS



Risky stem cell treatment reverses MS in 70% of patients in small study

Prenda lawyers lose key appeal, will pay $230k sanction

BEEP BEEP, WHO'S GOT THE KEYS TO MY SKYJEEP?

Can Google's Larry Page make flying cars a reality?

there's no connection between the two vulnerabilities.

Post updated to add link to original disclosure and detail about exploitability.

FURTHER READING

HUGE NUMBER OF SITES IMPERILED BY CRITICAL IMAGE-PROCESSING VULNERABILITY [UPDATED]

Attack code exploiting critical ImageMagick vulnerability expected within hours.

LINKEDIN RECS: JUNGLING, TOP LANING

***League of Legends* admits to using chat-log analysis in employee reviews**

Tesla denies suspension issue and accuses blogger of lying

FRIDAY DEALS

Dealmaster: Get a Dell Inspiron 15 7559 for $749.99

READER COMMENTS 27

- - -

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

SITE LINKS

About Us
Advertise with us
Contact Us
Reprints

SUBSCRIPTIONS

Subscribe to Ars

MORE READING

RSS Feeds
Newsletters

Visit Ars Technica UK

CONDE NAST SITES

Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE