


Zero-Day Exploit Found in Kaspersky Antivirus UPDATED

 Start searching now... 



Kaspersky quickly rolls out update to fix the issue

By Catalin Cimpanu  7 Sep 2015, 11:57 GMT

Tavis Ormandy, an Information Security Engineer at Google, has found a zero-day exploit in Kaspersky's antivirus product, as he announced on Twitter last Saturday.

According to Ormandy's tweet, the Google security researcher had found a zero-day exploit in Kaspersky's antivirus, versions 15.x and 16.x.

Later on he detailed the vulnerability as "a remote, zero interaction SYSTEM exploit, in default config."

Basically, the Kaspersky zero-day bug would have permitted an attacker to easily infiltrate the victim's computer, and gain system-level privileges, allowing him to carry on any kind of attacks without restrictions.

The Kaspersky team was very responsive to a tweet seeking contact with their security staff, even the company's president, Eugene Kaspersky, [getting involved](#) and making sure the vulnerability was properly and privately disclosed.

Kaspersky announced an update in less than 24 hours

One day later, on Sunday morning, Kaspersky announced a worldwide update for its product.

Since so little details were provided on Twitter, and Kaspersky released an update in less than 24 hours, there are small chances this vulnerability was ever used by any malicious actor.

This is not the first time Ormandy exposed a flaw in a security product, the Google engineer previously discovering and disclosing vulnerabilities in Sophos and ESET's antivirus engines. He also found a zero-day vulnerability in Windows XP's Help and Support Center.

Security researchers like Graham Cluley have been [highly critical](#) of Ormandy in the past because he doesn't seem to want to follow regular protocol when it comes to disclosing bugs to software manufacturers.

Instead, Ormandy just puts the information online, which can easily be picked up by hackers and integrated in exploit kits. This time, the details he provided were scarcer, and he seems to have followed the "unofficial" disclosure protocol.

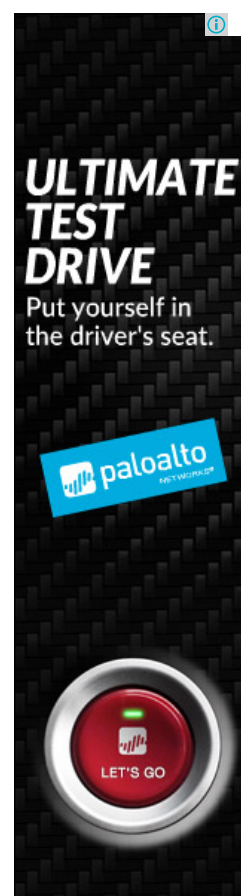
Softpedia reached out to Kaspersky and we'll update the article as new information comes to light.

UPDATE: Kaspersky Lab has answered Softpedia's inquiry into the matter with the following statement:

"We would like to thank Mr. Tavis Ormandy for reporting to us a buffer overflow vulnerability, which our specialists fixed within 24 hours of its disclosure. A fix has already been distributed via automatic updates to all our clients and customers. We're improving our mitigation strategies to prevent exploiting of inherent imperfections of our software in



 Kaspersky fixes zero-day bug



MORE ON THIS TOPIC




Study: Mobile Device Proliferation Is Causing Digital Amnesia



Carbanak Banking Trojan Returns with a New Series of Attacks

irm.exe2.544 K4.232 K644 Local Session Manager Serv...



Tavis Ormandy


@taviso

Follow

Okay, first Kaspersky exploit finished, works great on 15 and 16. Will mail report after dinner. /cc @ryanaraine

10:43 AM - 5 Sep 2015

413290



Tavis Ormandy

@taviso

Follow

Kaspersky tell me they're rolling out a fix globally right now, that was less than 24hrs.

10:50 AM - 6 Sep 2015

4238

#Kaspersky, #zero-day, #vulnerability, #Kaspersky Lab, #antivirus



Windows Server 2003

終止支援免驚

7/14 終止支援後

採用 Deep Security 虛擬補丁
解決資安漏洞、降低成本

了解更



Self-Driving Cars Are Hackable

MORE ON: SELF-DRIVING CAR

Hot right now

Latest news

This site uses cookies to offer you a complete experience. Find out more or CLOSE x this notification permanently.



New Nexus 5 (2015)
Press Render Shows
Right Edge of the
Smartphone



Apple's iPhone 7 to
Be 6 Millimeters
Thin



Microsoft's
Chairman Talks
About the New CEO,
Steve Ballmer,
Nokia Deal



Default Hard-Coded
Credentials Expose
Seagate Wireless
Hard Drives to
Attacks



Kaspersky Lab Systems Hit
by Cyber Attack with Duqu 2



Simplocker Android

MORE +

RELATED APPS



ZipKrypt

reliable
application designed to

FLASH SALE: BullGuard Internet Security 50% OFF!



Free RAR Password
Unlocker: Unlock encrypted
archived files, with this



Hide IP Speed: The perfect
tool for you if you're
concerned about Internet



Comodo Firewall: Browse

MORE +

http://news.softpedia.com/news/zero-day-exploit-found-in-kaspersky-antivirus-491086.shtml2/3

1 Comment



Share your thoughts on this story!



 SUBMIT

I ♥ SOFTPEDIA®

 Like

202K

 +1

56K

 Follow

13K

 Search here...

© 2001-2015 Softpedia. All rights reserved. Softpedia® and the Softpedia® logo are registered trademarks of SoftNews NET SRL. [Privacy Policy](#)