

[Home](#)

 [Subscribe](#)

« [Previous post in Support](#)



McAfee Response To Current False Positive Issue Wednesday, April 21st, 2010 at 4:29 pm by Barry McPherson

In the past 24 hours, McAfee identified a new threat that impacts Windows PCs. Researchers worked diligently to address this threat that attacks critical Windows system executables and buries itself deep into a computer's memory.

The research team created detection and removal to address this threat. The remediation passed our quality testing and was released with the 5958 virus definition file at 2.00 PM GMT+1 (6am Pacific Time) on Wednesday, April 21.

McAfee is aware that a number of customers have incurred a false positive error due to this release. Corporations who kept a feature called "Scan Processes on Enable" in McAfee VirusScan Enterprise disabled, as it is by default, were not affected.

Our initial investigation indicates that the error can result in moderate to significant issues on systems running Windows XP Service Pack 3.

The faulty update was removed from all McAfee download servers within hours, preventing any further impact on customers. We believe that this incident has impacted less than one half of one percent of our enterprise accounts globally and a fraction of that within the consumer base.

McAfee teams are working with the highest priority to support impacted customers. We have also worked swiftly and released an updated virus definition file (5959) within a few hours and are providing our customers detailed guidance on how to repair any impacted systems.

Corporate Customers

- These entries in our virus [information library](#) and the [knowledge base](#) provide workarounds for this issue for corporate customers

Consumers

- This support page provides information for [impacted consumers](#)

We are investigating how the incorrect detection made it into our DAT files and will take measures to prevent this from reoccurring.

The new 5959 virus definition file provides updated protection, including detection for the referenced new threat that attacks core Windows executables and buries itself deep into a computer's memory.

We sincerely apologize for the inconvenience this has caused our customers and will update this blog posting as more details become available.

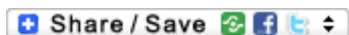
Barry

(Updated at 3.35 PM PT to include statement on number of customers impacted.)

(Updated at 3.50 PM with a link to details for consumers who were impacted.)

(Updated at 5.13 PM with link to knowledge base.)

(Updated at 5.44 PM to correct the number of impacted consumers.)



Tags: [mcafee](#), [Support](#)

- Posted in [Support](#)

Feeds & Podcasts

Meet the Bloggers

Archive

Categories

Blogroll

- [CNET Security News](#)
- [eWeek Security Watch](#)
- [Krebs On Security](#)
- [StorefrontBacktalk](#)
- [UnsafeBits](#)
- [Zero Day – ZDNet.com](#)

April 2010

S M T W T F S

1 2 3

4 5 6 7 8 9 10

11 12 13 14 15 16 17

18 19 20 21 22 23 24

25 26 27 28 29 30

[« Mar](#)



- [Security Insights Newsletter](#)



- [Security Insights on the Web](#)

- [About this blog](#)
- [View all posts by Barry McPherson](#)
- [View all posts in Support](#)

Submit your comment

 Name (required)

Mail (will not be published) (required)

Website

XHTML: You can use these tags: <abbr title=""> <acronym title=""> <blockquote cite=""> <code> <del datetime=""> <i> <q cite=""> <strike>



You must read and type the **5 chars** within **0..9** and **A..F**, and submit the form.

Oh no, I cannot read this. Please, generate a

The postings on this blog are the opinions of the individual posters and don't necessarily represent McAfee's position or opinion on this subject.

© 2009 McAfee, Inc. All rights reserved. E & O E