ENSILO
SILO YOUR DATA FROM THREAT ACTORS

MENU

DECEMBER 8, 2015 BY TOMER BITTON

You’re so predictable: the AV vulnerability that bypasses mitigations

Our research team exposed a critical security vulnerability appearing in various Anti-Virus (AV) products which has the potential to turn the Anti-Virus to an attack-enabler tool. This issue is not necessarily constrained to security solutions, but potentially to any intrusive application such as data leak prevention (DLP) and performance monitoring solutions.

Due to the pervasiveness of Anti-Virus products - a market valued at $3.5 billion, with about 400 million seats, this vulnerability potentially affects millions of Anti-Virus customers.

Background

While at a customer site in March 2015, the enSilo product alerted on a product collision with AVG, also installed in the customer’s environment. A follow-up investigation conducted by our researchers revealed a flaw in AVG which effectively enabled a threat actor to exploit any old vulnerability (for instance, as of 2010) in a 3rd party application (such as Acrobat Reader) in order to compromise the underlying Windows system.

We had responsibly disclosed this issue to AVG, and they had patched the vulnerability within two days of our notification.

The AVG finding prompted us to create a tool that tests other Anti-Virus products for this vulnerability in order to avoid any such future collisions.

The Vulnerability

The vulnerable Anti-Virus products allocate a memory page with Read, Write, Execute (RWX) permissions at a constant predictable address. This allocation occurs for various user-mode processes belonging to third party applications such as browsers and Adobe Reader.

As mentioned in our March AVG release, this flaw significantly diminishes the efforts that the threat actor needs in order to exploit a third party application. In turn, this can lead to the compromise of the underlying Windows system.

How? Microsoft places many Windows mitigations against exploits, for instance the randomization of memory (ASLR) and preventing data from running in memory (DEP). Since the memory page is at a constant predictable address, the attacker can know where to write and run the code. With the memory allocation set to RWX, that code can be executed, essentially defeating those hurdles that Windows placed in front of threat actors.

Vulnerable Products

For now we have found this vulnerability in the following Anti-Virus products. We'll continue updating this list as we receive more information.

- McAfee Virus scan Enterprise version 8.8. This vulnerability appears in their Anti Malware + Add-on Modules , scan engine version (32 bit) 5700.7163 , DAT version 7827.0000 , Buffer Overflow and Access Protection DAT version 659 , Installed patches: 4. We have notified McAfee and they have silently fixed it in their patch dated Aug. 20, 2015.
- Kaspersky Total Security 2015 - 15.0.2.361 - kts15.0.2.361en_7342. We have notified Kaspersky and they have silently fixed it in their patch dated Sept. 24, 2015.
- AVG Internet Security 2015 build 5736 + Virus database 8919. As mentioned above, AVG has released their patch on March 12th.

Given that this is a repetitive coding issue amongst Anti-Virus – an intrusive product, we believe that this vulnerability is also likely to appear in other intrusive products, non-security related, such as application-performing products.

Is my Computer Vulnerable?

Considering the gravity of this issue, we created a tool - AVulnerabilityChecker - that

checks whether an application running on your machine is vulnerable to this flaw. If vulnerable, AVulnerabilityChecker will not be able to tell you which application contains the flaw, but it will point out where to start the analysis.

Since the vulnerability manifests itself through a user-mode process, AVulnerabilityChecker performs these tests against the browser. It is important to note that although we use browsers to check this vulnerability – the vulnerability is not in the browser. However, we do provide the browser details as these are important for investigation. For more details on the tool's usage and follow-up analysis, see the technical breakdown here:

http://breakingmalware.com/vulnerabilities/sedating-watchdog-abusing-security-products-bypass-mitigations/

If you find a vulnerable application, please email us (contact "at" ensilo.com), tweet (@enSiloSec) and we'll add it to our list.

You can download AVulnerabilityChecker from here: https://github.com/BreakingMalware

The Exploitability Factor

Exploiting this vulnerability is not just a theoretical musing. A Sept. 22 disclosure by Tavis Ormandy from Google's Project Zero discusses a vulnerability he exposed. Tavis further showed how he was able to exploit this vulnerability through a similar vulnerability appearing in Kaspersky, where a RWX memory section was allocated in a predictable address.

These types of vulnerabilities clearly demonstrate the problems in the security eco-system. On the one hand, Microsoft invests loads of resources in defenses, mitigations and enhancements to strengthen its system against compromise. On the other hand, there'll always be some oversight in applications. Unfortunately, it's precisely vulnerable third party applications which can lead to the compromise of these same defenses.

Get Technical

A technical breakdown of this vulnerability appears here: http://breakingmalware.com/vulnerabilities/sedating-the-watchdog-abusing-security-products-to-bypass-mitigations

Mitigation

There are several steps we suggest taking:

- Run the offered tool on your device and see whether it is vulnerable or not.
  Due to the prevalence of this issue in AVs, we can assume that this issue is replicated across other intrusive applications (security and non-security related).
- Once you recognize that an application is vulnerable, we suggest you contact the affected vendor and understand from them how they plan on dealing with the issue.
- Operate as though your systems are already compromised.
  The industry has come to realize that vulnerabilities will continue to be present. A recent survey shows that on average 19 vulnerabilities are reported per day across applications. Unfortunately, there will always be threat actors looking out for them. Rather than playing the undefeatable game of "Whack-a-targeted-attack" against them, apply the necessary controls to ensure that the threat actors cannot achieve their goal of data exfiltration or tampering, even when the organizational environment is infected.

If you are an application developer, ensure that when allocating new code a) the code memory/allocation/buffer is allocated in a random location; b) the only permissions you grant to the new code is Read-Execute.

Update: This blog has been updated to reflect that we were notified that McAfee silently patched the vulnerability appearing in McAfee Virus Scan Enterprise 8.8.

POST TAGS WINDOWS, RESEARCH

Subscribe to enSilo's Blog and Stay on Top of the Latest Security Research and Industry News

Email*

SUBSCRIBE

Recent Posts

- You’re so predictable: the AV vulnerability that bypasses mitigations
- Cyber-Security in 120 Secs: POS Malware and the Cost of Breaches
- Cyber-Security in 120 Secs: Breaches Hit Hospitality and More
- Cyber-Security in 120 Secs: PoS Malware, FINRA Fines Scottrade
- Protecting VDI Environments from Exfiltration
- Cyber-Security in 120 Secs: Re-Invesigating Hacks and New Ransomware
- Cyber-Security in 120 Secs: FFIEC Warns on Attacks Involving Extortion
- Cyber-Security in 120 Secs: Damage Estimates for the TalkTalk Breach
- Cyber-Security in 120 Secs: Nation State Cyber-Espionage
- Ransomware Goes to Hollywood

Posts by Topic

- Weekly Security News (12)
- Research (8)
- Windows (5)
- Industry (4)
- Business (3)

Archive by Month

- October 2015 (7)
- November 2015 (5)
- September 2015 (3)
- March 2015 (2)
- April 2015 (2)
- June 2015 (2)
- December 2015 (2)
- February 2015 (1)
- July 2015 (1)
- August 2015 (1)