MUST READ AVG, McAfee, and Kaspersky antivirus were vulnerable to critical flaw

security affairs

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | Laws and regulations | Malware | Mobile | Data Breach | Security | Social Networks | Reports | EXTENDED COOKIE POLICY | Contact me |

igence Laws and

KIE POLICY Cont

AVG, McAfee, and Kaspersky antivirus were vulnerable to critical flaw

December 10, 2015 By Pierluigi Paganini

G+1 5

My Page Like 17

MORE S

Experts at enSilo have found a critical security vulnerability in various antivirus (AV) software that could be exploited by attackers to turn the AntiVirus to an attack-enabler tool.

Some of the most important security firms have had an ugly surprise, the security software they offer to their clints have been compromised by a serious vulnerability flaw that could be exploited to hack computers.

In March, the security researchers at enSilo firm discovered a serious vulnerability in the popul free antivirus engine AVG Internet Security 2015. The researchers discovered that the software allocating memory for read, write, and execute (RWX) permissions in a predictable address. The

alicious c

enSilo reported the vulnerability to AVG that promptly fixed it within a couple of days. The experts at enSilo decided to analyze other software commercialized by the principal security firms, including McAfee and Kaspersky.

They discovered that VirusScan Enterprise version 8.8 and Kaspersky Total Security 2015 were also affected by the vulnerability. Below the list of vulnerable products discovered by the experts:

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

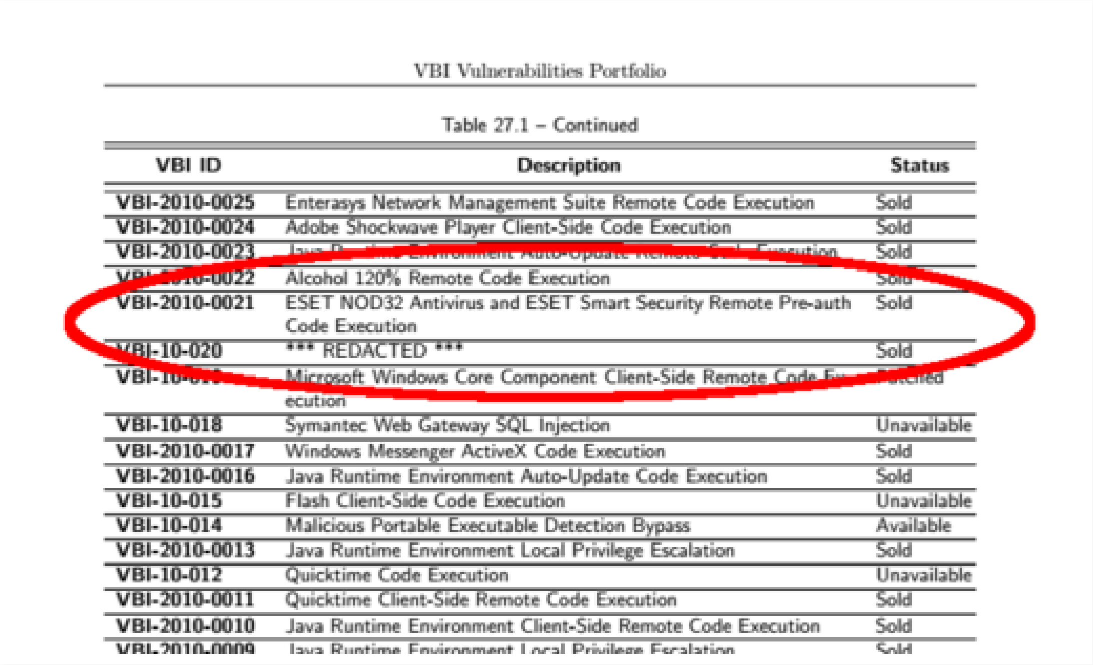
- *McAfee Virus scan Enterprise version 8.8. This vulnerability appears in their* Anti Malware *+ Add-on* Modules *, scan engine version (32 bit)* 5700.7163 *, DAT version* 7827.0000 *, Buffer Overflow and Access Protection DAT version 659 , Installed patches: 4. We have notified McAfee and they have 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.*

The researchers plan to analyze other solutions and update the readers about the status of their security software.

"We'll continue updating this list as we receive more information," said Tomer Bitton, VP of research at enSilo, in a blog post.

"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."

Other experts wrote about the security issue, Tavis Ormandy, security expert at Google, has written about a similar issue with Kaspersky software. In the blog post the hacker detailed how it is possible to exploit the security issue.



VBI Vulnerabilities Portfolio

Table 27.1 – Continued

VBI ID	Description	Status
VBI-2010-0025	Enterasys Network Management Suite Remote Code Execution	Sold
VBI-2010-0024	Adobe Shockwave Player Client-Side Code Execution	Sold
VBI-2010-0023	Java Runtime Environment Auto-Update Remote Code Execution	Sold
VBI-2010-0022	Alcohol 120% Remote Code Execution	Sold
VBI-2010-0021	ESET NOD32 Antivirus and ESET Smart Security Remote Pre-auth Code Execution	Sold
VBI-10-020	*** REDACTED ***	Sold
VBI-10-019	Microsoft Windows Core Component Client-Side Remote Code Execution	Patched
VBI-10-018	Symantec Web Gateway SQL Injection	Unavailable
VBI-2010-0017	Windows Messenger ActiveX Code Execution	Sold
VBI-2010-0016	Java Runtime Environment Auto-Update Code Execution	Sold
VBI-10-015	Flash Client-Side Code Execution	Unavailable
VBI-10-014	Malicious Portable Executable Detection Bypass	Available
VBI-2010-0013	Java Runtime Environment Local Privilege Escalation	Sold
VBI-10-012	Quicktime Code Execution	Unavailable
VBI-2010-0011	Quicktime Client-Side Remote Code Execution	Sold
VBI-2010-0010	Java Runtime Environment Client-Side Remote Code Execution	Sold
VBI-2010-0009	Java Runtime Environment Local Privilege Escalation	Sold

Snippet of an exploit pricelist uncovered by WikiLeaks, source. The pricelist demonstrates that anti virus exploits and information are actively traded.

Considering the gravity of the problem and its widespread nature, enSilo has created a free checking tool called AVulnerabilityChecker to allow users checking if their machine is 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." states enSilo.

McAfee and Kaspersky have already fixed the security issue.

Pierluigi Paganini

(Security Affairs – antivirus software, Internet Root servers)

Share it please ...

Hacking antivirus McAfee Kaspersky Pierluigi Paganini Security Affairs AVG security software

Breaking News Hacking Security

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

NCA launched #CyberChoice campaign, to prevent youngsters become cyber criminals

YOU MIGHT ALSO LIKE

Internet root servers flooded with 5 million queries a second

December 10, 2015 By Pierluigi Paganini

xboxlive digital certificate exposed opens users to MITM attacks

December 9, 2015 By Pierluigi Paganini