# Reaction to McAfee Statement

*regarding vulnerabilities in Anti-Virus Software*

**Thierry Zoller**
Thierry.Zoller@nruns.com
Senior Senior Security Engineer, n.runs AG

n.runs professionals

n.runs AG is a vendor-independent consulting company specializing in the areas of: IT Infrastructure, IT Security ,IT Business Consulting and IT Applications. For additional information visit the n.runs AG website at www.nruns.com.

*n.runs recently announced that they discovered over 800 vulnerabilities in AV software, blaming a necessary procedure that is known as parsing. McAfee reacted by posting a statement to the McAfee Avert blog[1], n.runs would like to take the opportunity and react to these statements. For more information about the original press-release please refer to http://www.nruns.com/_en/aps/press.php*

As a Senior Security Engineer I also support the Product Management from the security side and as such I felt entitled to comment on the response by McAfee[2]. Firstly, before I start, n.runs would like to thank McAfee for the cooperation on vulnerability disclosure and quick and professional reaction to vulnerability notifications.

Ryan Permeh writes:

> "The ZDNet posting includes scary graphs to frighten users of security products."

We would like to clarify the statistics those graphs are based on were gathered using an independent database from Secunia and National Vulnerability Database, ZDnet has not produced them. Secunia and the National Vulnerability Database are trusted and respected aggregators of security vulnerabilities and advisories and provided the database to these statistics. Let us emphasize that the intention was not to scare as the statement from McAfee implies, but to put independent facts in addition to those from n.runs on the table. The statistics show a vendor independent view on AV vulnerabilities.

> "We researched the N.Runs claims by analyzing the raw data and found their claims to be somewhat exaggerated."

n.runs would also like to clarify that researching the "N.Runs claims" is an impossible task for McAfee as the number 800 (actually it's more than this now) is the result of ALL vulnerabilities reported **by n.runs** to AV vendors. McAfee has no knowledge of many of these. These are either not publicly known yet and/or are in the process of being patched. The number 227 as also displayed on our website is the number of AV vulnerabilities that were present from 2001 to 2007 in AV software according to statistics generated by using Secunia 's database.

> "We don't want to attack the legitimacy of the vulnerabilities they found, but do call into question the conclusions drawn on what this means to the state of security."„The press release is essentially a sales pitch for their upcoming product, APS-AV. This is a new product without much real world exposure that itself has yet to be scrutinized by the security researcher community."

aps-AV is in fact not an upcoming product, but is already available.. It has also been reviewed by the very same people who found these 800 AV bugs as well as some of our best source code auditors. The architecture revolves around the concept that whatever the AV Products do, either intentionally (backdoor) or unintentionally (flaw) they cannot harm the security requirements of the environment they run in. The concept and design for aps-AV were developed in conjunction with Felix "FX" Lindner of Recurity Labs.

---

1 http://www.avertlabs.com/research/blog/index.php/2008/07/10/vulnerabilities-in-av-software/

2 http://vil.nai.com/images/AvertBlog_Vulnerabilities%20in%20AV%20software.pdf

> "All successful vendors are used to this threat and have processes to quickly deal with such bypass issues."

This is unfortunately not the case. Some vendors fix bypass issues within 1 week, while others (including some with very significant market share) take up to 2.5years. n.runs believes that waiting until a bypass is actively used by malware prior to patching this flaw is leaving a door open for attackers.

> "One of the conclusions drawn by N.Runs is that having AV in your environment makes you less secure than not having it at all."

We would like to **emphasize this is clearly not what n.runs believes.**We are convinced that AV software is necessary and a requirement for today's security defense. What n.runs believes is that **multiple engines increase the chance of parsing bugs to occur**. Let us show what we mean by using anexample based on an Email setup *(Detection rates are examples, attack surface in this case is represented by the number of formats supported, # of vulnerabilities per format is an estimate based on our audits).*

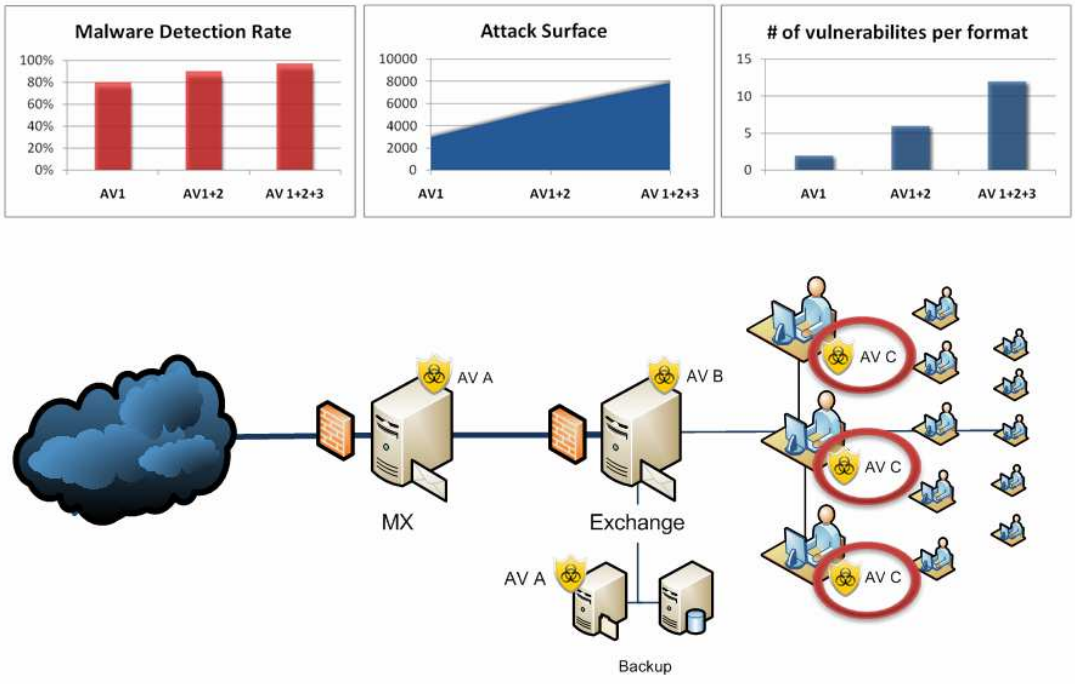



**Figure 1 - Attack surface increase | Example**

E-mail is being routed through all three engines, the detection rate increases as does the remotely reachable attack surface.

**n.runs firmly believes that the use of AV software or even multiple AV software is a requirement as of today**, but that the inherent bugs of AV Software need to be taken into account when designing your perimeter and internal security defense. The rising number of available formats, cryptors, packers combined with the intrinsic market pressure in the AV field (release early, release often) has not helped AV Vendors to increase code quality over the years, as the very same statistics and our experience over the years have clearly indicated (more on this later).We are convinced that AV vendors should focus on doing what AV vendors do best : Recognize malware, aps-AV takes care of the rest.

> "In addition, McAfee has not seen any evidence of any of the vulnerabilities reported by N.Runs being exploited to attack our products in real world environments."

This is due to the fact that n.runs reports these vulnerabilities in order to protect our own and McAfee customers. Our vulnerability notification policy is rigid and strict, advisories included no details as to how the vulnerability was found or how it could be exploited.In our view, the bigger concern are those vulnerabilities not found and published by us, especially as black-market prices for AV-vulnerabilities are on the rise. n.runs is aware of two publicly documented incidents where AV software (running on E-mail servers) was the remote entry vector to internal networks. **n.runs also believes that security is a process aimed at being proactive and not solely a process in reaction to events or bugs**. Statements such as "McAfee has not seen any evidence" can be deceptive.

For instance, Immunity explained in great detail how they penetrated an Enterprise over AV software on an MTA and used it to covertly shuffle data in and out over weeks. They further explain why they choose AV Software and not a web server or client-side exploits. The attack was done in a similar way to how a professional attacker would proceed., They replicated the existing infrastructure and searched for exploitable conditions and they found one. We do think this backs up our views of the actual threat posed by vulnerabilities in AV software.

The logic that bugs are fixed when they are found is no argument against a professional attacker for the sole reason that these professional and/or military style attackers rarely use known flaws. If the paradigm you follow is – "we protect against what is known" (quite common in the AV industry) then you are doing no favor to those who demand protection against professional attackers.

> "There is no silver bullet to software security. Getting to secure code is challenging. This involves proper software security practices including threat modeling, code auditing, and intensive security testing."

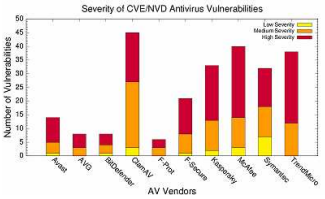
n.runs welcomes the AV-Industry SDL (Secure Development Lifecycle) effort spearheaded by McAfee. While we greatly support the introduction of an SDL, it will not entirely extinguish flaws with security relevance. Although it has the potential of greatly reducing their number and impact, it will not lead to invulnerable software.

In order to reach this goal, we consider it necessary to reduce the amount of trusted code to an absolute minimum, reduce the attack surface to an absolute minimum and place all untrusted code into a strictly confined environment, where no matter how badly the code behaves, no matter how many vulnerabilities it has, it cannot violate the security requirements.

This paradigm is what was brought to life with aps-AV.

> "I would like to discuss some of the actual numbers behind some of the claims made by N.Runs. One graph that quickly caught my eye came from an analysis of antimalware vulnerabilities published by University of Michigan researchers in Q1, 2008."

n.runs would like to clarify that the graph in question is the result of research by Jon Oberheide, Evan Cooke, Farnam Jahanian / *Electrical Engineering and Computer Science Department* of the University of Michigan. The research was cosponsored by the Department of Homeland Security (DHS) and the National Science Foundation.



> ”As manager of product security, I have insight into all vulnerabilities found in McAfee products. The raw number of McAfee vulnerabilities shown in this graph as about 40 seemed exceptionally high, so I did some deeper research. [..] I used a search for “McAfee and virus” in the search engine for NVD and came up with 37 findings. ”

While n.runs is unsure how the university came up with exactly these figures, we would have loved to see the results of the internal “insight into all vulnerabilities” and not an incomplete third party dataset of publicly known vulnerabilities which does not include the pending vulnerability reports (more on this later). We consider unpublished security bugs significant threats, since the exposure window can be quite high and the probability that someone else also discovers the same flaw is increasing these days. There are entire companies doing nothing else than researching vulnerabilities or reversing patches to find the fixed vulnerabilities.

> ”It is also important to understand the CVSS scoring mechanism. CVSS has many factors involved in the computation of that score. Some of the key factors involved are the impact of the vulnerability upon successful attack and the potential for exploitability of the vulnerability”

n.runs took the Excel file provided by McAfee that represents the base to the graphs and conclusions presented in the PDF. First of all, vulnerabilities **that have not yet been patched and are pending are not included in the list.** The list is purely based on information found on the Internet. Furthermore, n.runs was a mildly surprised by how the temporal scores were calculated. Many bugs had readily available PoC code yet were downgraded to scores of LOW or MEDIUM. Here is the scoring revisited with information found on Securityfocus, Milw0rm, Secunia, CVE, MITRE. The ratings are commented with links to PoC code. During this review, n.runs also noticed some odd ratings from NVD themselves, for example rating a remotely exploitable condition as local.

| CVE | Year Published | CVSS - offical | | CVSS - (Mcafee) | | CVSS (nruns) | Product |
|---|---|---|---|---|---|---|---|
| CVE-2007-2584 | 2007 | 10 | high | 6,7 | h | **8,3** | Consumer |
| CVE-2007-2152 | 2007 | 7,9 | high | 5,8 | m | 5,8 | **VSE** |
| CVE-2007-1538 | 2007 | 7,5 | high | 3,3 | l | 3,3 | VSE |
| CVE-2007-1227 | 2007 | 4,1 | medium | 3 | l | **3,4** | Virex |
| CVE-2007-1226 | 2007 | 4,1 | medium | 3 | l | **5,6** | Virex |
| CVE-2006-6474 | 2006 | 4,6 | medium | 3,5 | l | **3,5** | VSE - linux |
| CVE-2006-5417 | 2006 | 5 | medium | 3,9 | l | 3,9 | Consumer |
| CVE-2006-4886 | 2006 | 3,7 | low | 2,5 | l | 2,5 | VSE |
| CVE-2006-3961 | 2006 | 7,5 | high | 5,5 | m | **6,2** | Consumer |
| CVE-2006-3575 | 2006 | 2,1 | low | 1,5 | l | **1,8** | VSE |
| CVE-2006-0982 | 2006 | 5 | medium | 4,3 | m | **5** | Virex |
| CVE-2005-4505 | 2005 | 7,2 | high | 5,6 | m | **6,3** | VSE |
| CVE-2005-3657 | 2005 | 5 | medium | 3,9 | l | **3,7** | Consumer |
| CVE-2005-3377 | 2005 | 5,1 | medium | 4 | m | **4,2** | Engine |
| CVE-2005-3215 | 2005 | 5,1 | medium | 4 | m | 4 | Engine |
| CVE-2005-0644 | 2005 | 7,5 | high | 5,9 | m | **6,2** | Engine |
| CVE-2005-0643 | 2005 | 7,5 | high | 5,9 | m | **6,2** | Engine |
| CVE-2004-0932 | 2005 | 7,5 | high | 5,9 | m | **6,2** | Engine |

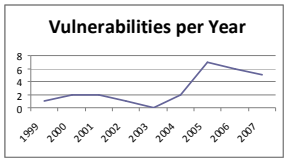
**Figure 2 - CVSS McAfee adjustments revisited**

We would also like to note that lowering the rating after the patch is available makes sense, but leaves the exposure window and usage of these flaws to penetrate targets completely out of the calculation. This is why aps-AV is proactive in the sense that code execution and bypasses simply have no consequences.

> "The interesting fact is that only five of the 26 vulnerabilities even fell within the area the N.Runs was testing for and where their product could possibly protect a user."

n.runs would like to clarify that McAfee is not aware of the nature and feature set of aps-AV ("their product") and as such cannot judge where and how aps-AV protects enterprises. aps-AV does a lot more than just protect against unknown attacks against AV solutions - it allows to break out of vendor lock-in and use as many AV Engines as you wish without being tied to them, it allows to swap them by pressing a button and much more[3].

> "Our numbers seemed to have peaked in 2005, which is contrary to the trending that the N.Runs reports."



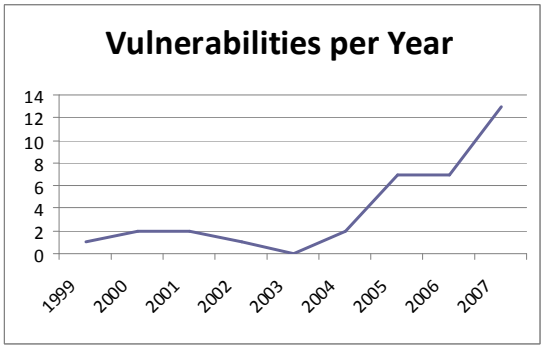

n.runs finds it astounding that McAfee comes to this conclusion without taking the vulnerabilities into account that have been reported but where the patch is still pending - and without taking into account the vulnerabilities listed for example on secunia, which are not listed in CVE.

n.runs has the following bugs pending and is aware of at least another DoS bug pending from a independent researcher. **Here is the list of pending McAfee bugs reported by n.runs :**

Incident ID: MFE-FW-20060227-01 - Date of receipt: February 27, 2006
Incident ID: MFE-ENG-20070605-01 - Date of receipt: June 5, 2007 (Possible Vuln #15)
Incident ID: MFE-ENG-20070607-01 - Date of receipt: June 7, 2007 (Possible Vuln #18)
Incident ID: MFE-ENG-20070608-01 - Date of receipt: June 7, 2007 (Possible Vuln #23)
Incident ID: MFE-ENG-20070608-02 - Date of receipt: June 7, 2007 (Possible Vuln #25)
Incident ID: MFE-ENG-20070615-01 - Date of receipt: June 15, 2007 (Possible Vuln #27)
Incident ID: MFE-ENG-20070615-02 - Date of receipt: June 15, 2007 (Possible Vuln #28)
Incident ID: MFE-ENG-20071111-01 - Date of receipt: November 11, 2007 (Possible Vuln #36)
Incident ID: MFE-ENG-20071111-02 - Date of receipt: November 11, 2007 (Possible Vuln #37)

Simply adding these pending reports to the graph gives the following result. n.runs believes this does indeed represent a trend, not to mention these only include problems reported by n.runs, not external researchers or entities nor internal penetration test efforts (which also pose a security threat during the exposure window but are never published).

| Year Breakdown | |
|---|---|
| 1999 | 1 |
| 2000 | 2 |
| 2001 | 2 |
| 2002 | 1 |
| 2003 | 0 |
| 2004 | 2 |
| 2005 | 7 |
| 2006 | 7 |
| 2007 | 14 |




[3] http://www.nruns.com/_en/aps/aps-description.pdf

> "This blog is just an attempt at putting things in perspective. FUD and skewed reporting backed by marketing driven press releases do not help."

n.runs wants to underline that we also believe FUD does not help. This is why we invest a lot of time in coordinating responsible disclosure with up to 13 vendors for one bug (even simple ones). These procedures take a lot of time and resources, which is also the reason why not more of these bugs have been publicly posted. If one vendor takes over 2 years to patch,we wait 2 years until we publicly disclose the flaw, even if the other vendors patched within a week. We could leverage more FUD by releasing PoC files and more details, but we have so far abstained from doing so.

> [..]"McAfee are doing the right thing in reducing risk for our customers and presenting the best possible level of security."

n.runs believes the best possible level of security is one where no patches are required to guarantee the highest possible level of security.

## *About n.runs*

n.runs AG is a **vendor-independent** consulting company specializing in the areas of: IT Infrastructure, IT Security and IT Business Consulting. In 2007, n.runs expanded its core business area, which until then had been project based consulting, to include the development of specialized security solutions.

## *About aps-AV®*

n.runs aps-AV® (Application Protection System Anti-Virus) is part of the n.runs aps product line. aps-AV® offers comprehensive E-Mail and Anti-virus protection by implementing the Defense-In-Depth-Principle in a high-secure 3-Tier architecture. aps-AV® not only offers multi-engine protection and the possibility of centralization but encloses the AV engines within a sealed environment. Additionally aps-AV® optimizes the performance of the servers and simplifies the administration of multiple AV engines and resources.
For more information please see: http://www.nruns.com/_en/aps/aps-description.pdf and http://www.nruns.com/_en/aps