

Vulnerabilities in AV software

A recent ZDnet blog (<http://blogs.zdnet.com/security/?p=1445>) discusses a large number of vulnerabilities German research team N.Runs says it found in antimalware products from nearly every vendor. The ZDNet posting includes scary graphs to frighten users of security products. We researched the N.Runs claims by analyzing the raw data and found their claims to be somewhat exaggerated.

First, N.Runs has indeed found many vulnerabilities and they deserve credit for that. We have worked with the N.Runs team in the past and have found them to be very responsible and intelligent researchers. 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 ZDnet blog posting is based on a press release from the N.Runs team. 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.

While several of the bugs N.Runs found and publicly reported could result in remote code execution or denial of service, a large number of the vulnerabilities merely allow bypass of a certain type of detection. These bypass vulnerabilities present a much lower risk. In fact, every antimalware vendor has spent years dealing with malware writers who found clever ways around protection. All successful vendors are used to this threat and have processes to quickly deal with such bypass issues. In many cases bypasses only pose a real risk when an organization relies solely on malware protection at the edge of a network, for example in a gateway appliance. If best practices are followed and protections are layered throughout an organization, these threats will be blocked once the malware tries to do anything bad on the properly secured endpoints.

Still, the fact that N.Runs found many vulnerabilities in antimalware software is disturbing. It demonstrates that the security industry needs to focus its efforts on the practices of secure coding. Much like any other software, security vendors need to focus on writing clean, safe code

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.

Here at McAfee, we do all of this and more. We have baked security into our software development process. We use both automated and hand auditing techniques. We train our developers in secure code practices. We use fuzzers and perform penetration tests on our own software. This does not make us immune to software issues, but it has noticeably reduced the frequency and severity of vulnerabilities that are found.

N.Runs set out to find large numbers of vulnerabilities and it succeeded. Do keep in mind that the large number covers around 20 vendors, with some faring much worse than others in numbers of vulnerabilities found and severity of those vulnerabilities.

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. This concept is shortsighted. It is true that any software added to a system does

increase its complexity and often its attack surface. However, antimalware software protects millions of machines from thousands of unique and very active threats every day. In fact, McAfee products have prevented over 300 million infections in the last week alone

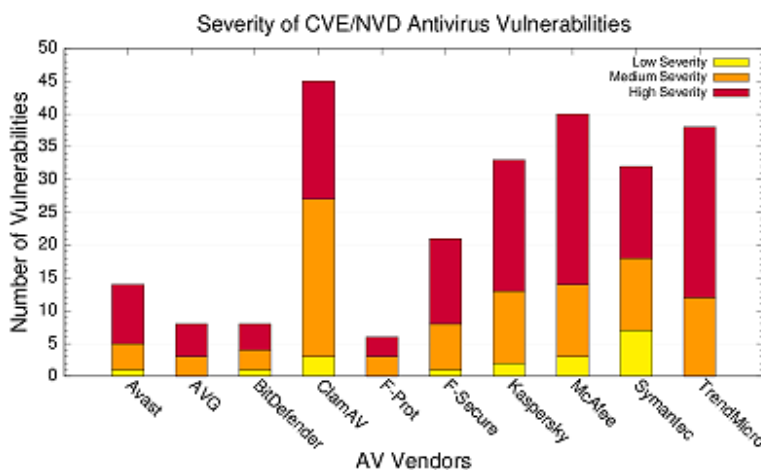
(http://vil.mcafee.com/mast/viruses_by_continent_internal.asp?continent_k=0&track_by=1&period_id=2). In addition, McAfee has not seen any evidence of any of the vulnerabilities reported by N.Runs being exploited to attack our products in real world environments.

Antimalware software closes holes in network architectures. Having security software correctly installed as a part of a layered network defense measurably reduces risk. By removing protection, a network is exposed to a constant stream of attacks that will go on forever.

Crunching the numbers

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. I am still looking for the original paper to back this graph up but have not yet been able to locate it. This only allows me to speculate on how the researcher gathered the data by using details in the graph itself.

AV-Vulnerabilities Q1/2008 - Source: University of Michigan

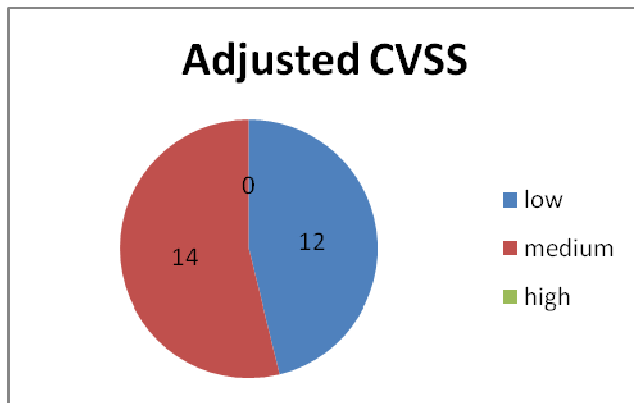
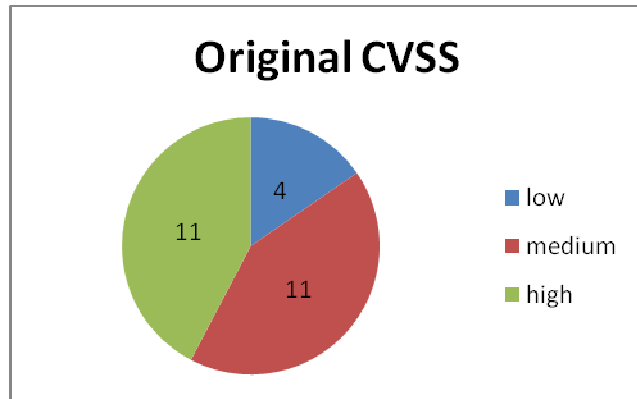


I am assuming the researchers are using data from the CVE/NVD

(Common vulnerability Enumeration / National Vulnerability Database) database at <http://nvd.nist.gov/>. This database tracks vulnerabilities and includes a CVSS (Common Vulnerability Scoring System) number for each of the found vulnerabilities. In the case of McAfee vulnerabilities the CVE database goes as far back as 1999. NVD maintainers assign a Low, Medium, or High severity CVSS score to each vulnerability. From the NVD site:

1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

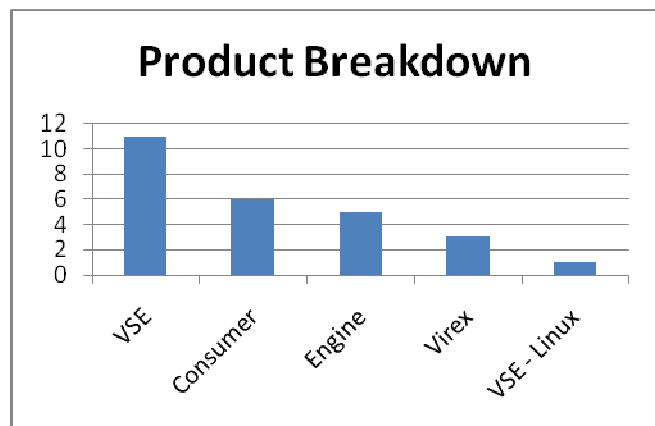
As manager of product security, I have insight into all vulnerabilities found in McAfee products. The raw number of McAfee vulnerabilities shown in this graph as about 40 seemed exceptionally high, so I did some deeper research. I anticipated that the University of Michigan researchers had incorrect data in the database or used a broad search term to determine the number of vulnerabilities. I used a search for “McAfee and virus” in the search engine for NVD and came up with 37 findings. From this 37, I found that 11 of these had absolutely nothing to do with McAfee products, bringing the number to 26. Of these 26, there were 11 high, 11 medium, and 4 low vulnerabilities. This is not what the N.Runs supplied graph shows, either in number of vulnerabilities or severity of those vulnerabilities. I further analyzed these results to see if the comparison is valid in showing graphs like this.



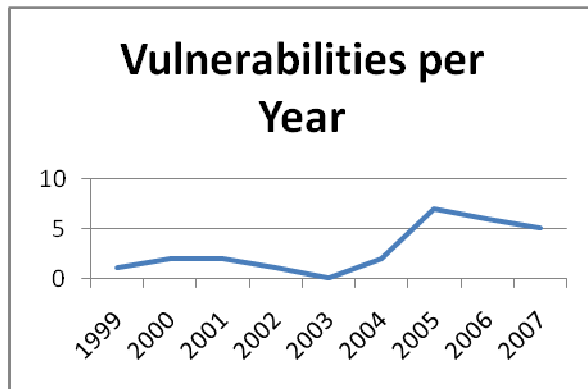
It is also important to understand the CVSS scoring mechanism. CVSS has many factors involved in the computation of that score. Some of the key factors involved are the impact of the vulnerability upon successful attack and the potential for exploitability of the vulnerability. CVSS has two other major modifiers. One is environmental, meaning how much it affects your specific environment. Another is temporal, which adjusts the score based on the availability

of an exploit and a vendor’s response. While environmental modifiers are specific to each user’s environment, we can correctly calculate the temporal scores. In doing this, I found a drastically adjusted set of scores, mostly by determining which issues were confirmed, which had official fixes, and which had ready exploits. I was even generous in these calculations, allowing for proof of concept exploits in situations where we had no proof that one existed. Upon completing the temporal adjustments, the breakdown was: 26 vulnerabilities, 0 high, 14 medium, and 12 low.

Additionally, I would like to point out that those 26 vulnerabilities were spread across five McAfee products. McAfee has a variety of products for consumers and corporations. These products work on a variety of platforms. The types of vulnerabilities also varied greatly, from weak registry keys to code execution. 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. The average severity of these five bugs was 6.54 before adjustments and 5.14 after accounting for temporal adjustments.



Finally, McAfee has been in the antimalware game for a long time. Since this report seems to span time, I thought I would offer a breakdown of vulnerabilities for McAfee broken down by year. Our numbers seemed to have peaked in 2005, which is contrary to the trending that the N.Runs reports.

From the data presented, we can make some pretty specific conclusions. From the numbers, it seems as if there is a discrepancy in how this is being

portrayed. Although we only took a look at the McAfee numbers, It doesn't quite come out to what N.Runs and the ZDnet blog entry implies.

Don't mistake this as a screed against security researchers. Responsible researchers looking for vulnerabilities in software are doing important work. In fact, N.Runs' research is important. Good researchers force software to get better. This blog is just an attempt at putting things in perspective. FUD and skewed reporting backed by marketing driven press releases do not help.

Even though there are vulnerabilities found in software, including security software, proactive vendors like McAfee are doing the right thing in reducing risk for our customers and presenting the best possible level of security.