

TOP 10 Vulnerability Trends for 2008

By Nevis Labs

Date: December 11, 2007



It's the last month of 2007 and the time is right to look back at the year and predict the vulnerability trends for 2008.

A quick glance at the National Vulnerability Database reveals that there has been a disclosure of 5,877 unique vulnerabilities so far this year.

Nevis Labs has been researching these and developing novel solutions to protect its customers.

Based on our research and documented information, the following are our predictions for the TOP 10 vulnerability trends in 2008:

- ActiveX
- File Format
- Antivirus
- Firewall
- IM
- Virtualization
- VISTA
- Driver
- VOIP
- Mobile

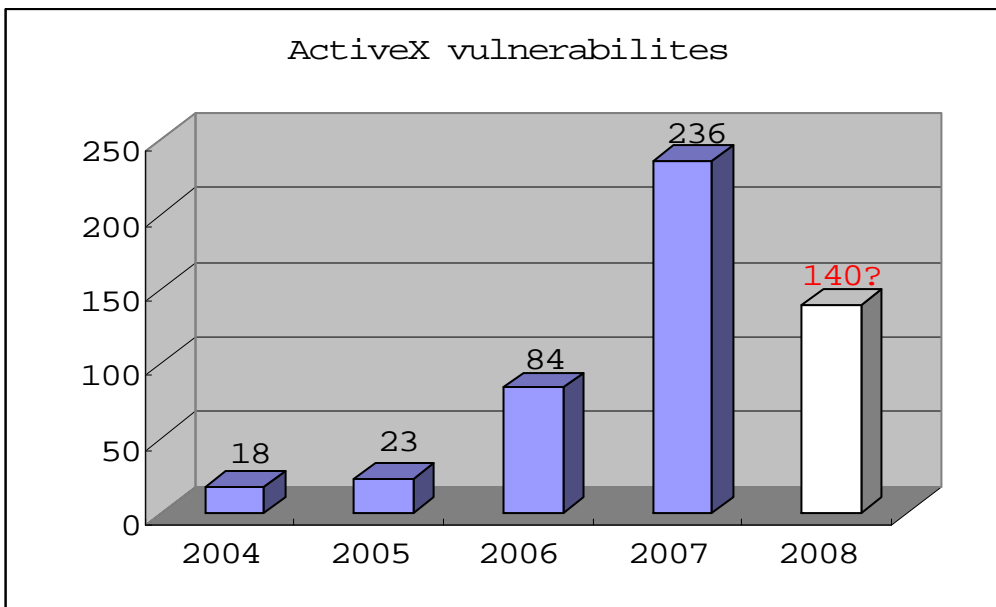
1 ActiveX

ActiveX-based vulnerabilities became more prevalent in 2007 than ever. We have seen ActiveX vulnerabilities being published every day, without a patch -- from Microsoft Internet Explorer to popular third-party applications.

There are two reasons for this:

- a) The popularity of the ActiveX fuzzing tools
- b) Exploiting ActiveX based vulnerabilities can be as easy as copying and pasting the vulnerable CLSID to the publicly available exploit template.

However, we expect a 30-40 per cent reduction in ActiveX based vulnerabilities being discovered and published in 2008 as compared to 2007.



[National Vulnerability Database](#)

It might be worth mentioning that because of the heavy use of JavaScript obfuscation techniques, there is no perfect solution as yet from IPS/IDS vendors for web browser-based vulnerabilities.

2 File Format

File-format-based vulnerabilities were one of the biggest headaches for both enterprise and security vendors in 2006 and 2007.

You may recall that there was at least one Microsoft Office ZERO-DAY exploit being captured in the wild in the second quarter of 2006?

Since REAL Remote vulnerabilities are getting rare, Client-side vulnerabilities have attracted the attention of both researchers and malicious hackers. File-format vulnerabilities are one of the main sources of client-side vulnerabilities, along with the ActiveX vulnerabilities discussed above.

The file formats which interest researchers the most are Microsoft Word, Excel, PowerPoint, Adobe Flash, Adobe Acrobat, Firefox, MSIE, QuickTime and RealPlayer. Additionally, some server-side file format problems exist, such as Microsoft Exchange and IBM Lotus.

We believe that file format vulnerabilities will still be popular in 2008, but the focus will move from Microsoft Office to Adobe products and other popular third-party applications.

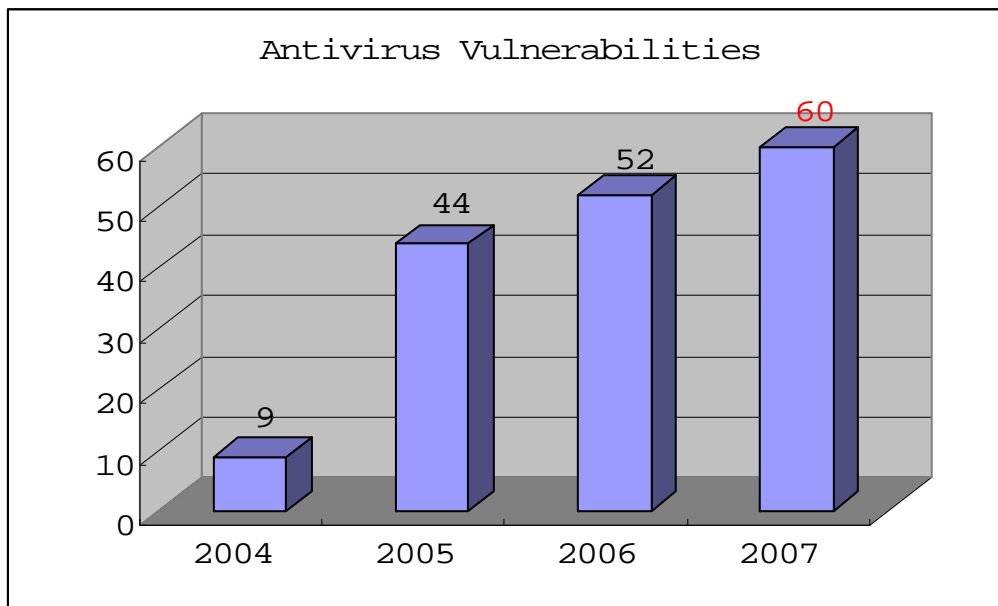
3 Antivirus

Since 2005, security researchers have focused on anti-virus vulnerabilities, and we have seen a dramatic increase of the AV vulnerabilities each year.

However, the methodology has changed. Fuzzing makes things much easier and actually leads to massive disclosures of AV vulnerabilities.

There will be again a steady increase in the number of the AV vulnerabilities being discovered in 2008.

More and more consumers will realize that Anti-virus software brings them both security and new vulnerabilities.



[National Vulnerability Database](#)

Even though there were dozens of AV vulnerabilities published, we saw very few exploits released and even proof-of-concept code is rare. Needless to say, there have been very few real world cases where AV vulnerabilities were exploited.

All the same, we believe there will be more and more AV vulnerabilities used for real world hacking.

4 Firewall

Since researchers and attackers are paying more attention to the security software, personal firewalls will be another important target.

Pure Antivirus solutions are not sufficient anymore. Most AV vendors have introduced an “Internet security suite”, thus making a personal firewall a must-have for home users.

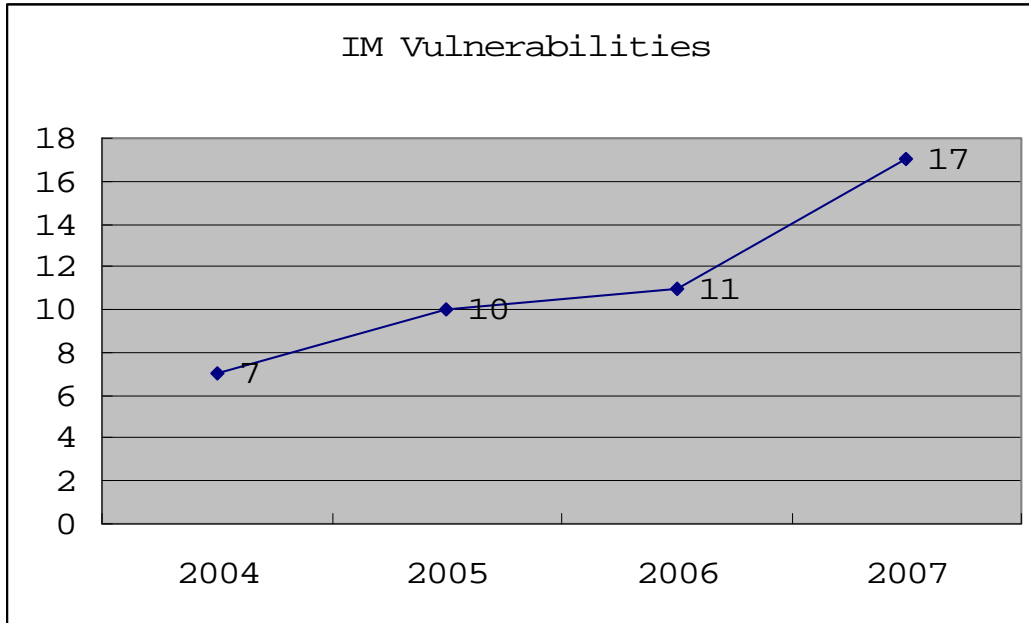
We therefore expect to see more firewall vulnerabilities, and more security software vulnerabilities, in 2008.

5 IM (Instant Messenger)

Instant messaging applications are becoming increasingly popular. According to the IDC, there will be more than 506 million people using instant messaging by the end of 2008.

Unfortunately, they are increasingly becoming the target of attackers, which places enterprises at risk from hackers, worms, and legal liabilities.

Related vulnerabilities focus on the image, audio, and video processing components.



Critical IM Vulnerabilities

We expect a rise in IM vulnerabilities too in 2008.

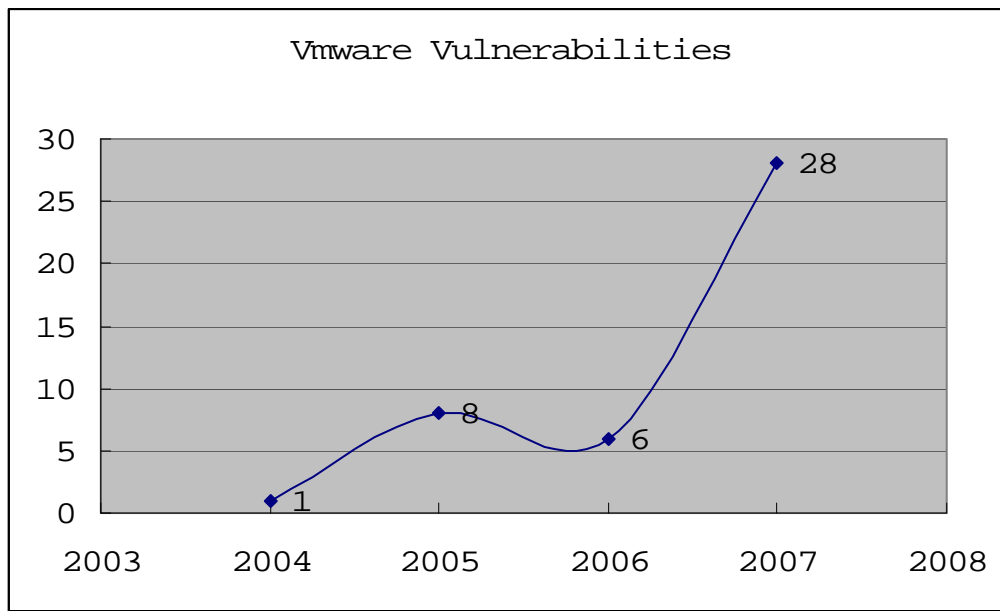
6 Virtualization

Virtual machines are a very popular vulnerability category, especially among security researchers.

Security researchers usually run unknown code within virtual machines because VM (Guest OS) is supposed to isolate the risk from their own computer (Host OS).

However, the attackers are paying more attention to the virtualization technology. It's not just about evading detections, the attackers are now trying to climb out of the VM, and root the Host OS!

Since people are paying more attention to this category, there will be more serious vulnerabilities uncovered here in the near future.



Vulnerabilities of VMware, market leader of the Virtualization

7 Vista

There were 27 CVE entries after Microsoft shipped the first patch for Vista in Jan., 2006. Vista looks much better when compared to other operating systems such as Windows XP.

Of course, the number of disclosed vulnerabilities alone is not a good indicator.

Another improvement is that there has not been a REAL Remote code execution vulnerability published for Vista thus far, which is absolutely a good record.

With an increase in Vista's market share, we also expect to see an increase in attacks and vulnerabilities being exposed Vista in 2008.

8 Driver

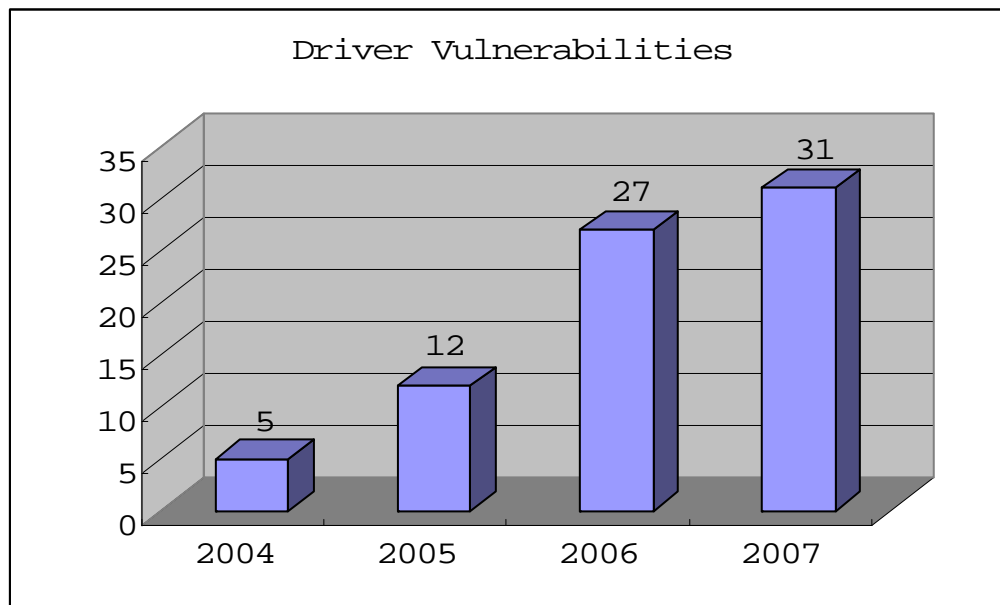
Driver vulnerabilities will grow steadily and will become more prevalent in 2008.

Vulnerabilities are concentrated in Antivirus software, firewall software, and wireless drivers. Most of these were introduced due to the following reasons:

- IOCTL handler Insufficient input verification
- SSDT hook. Insufficient Parameters validation of certain hooked functions.

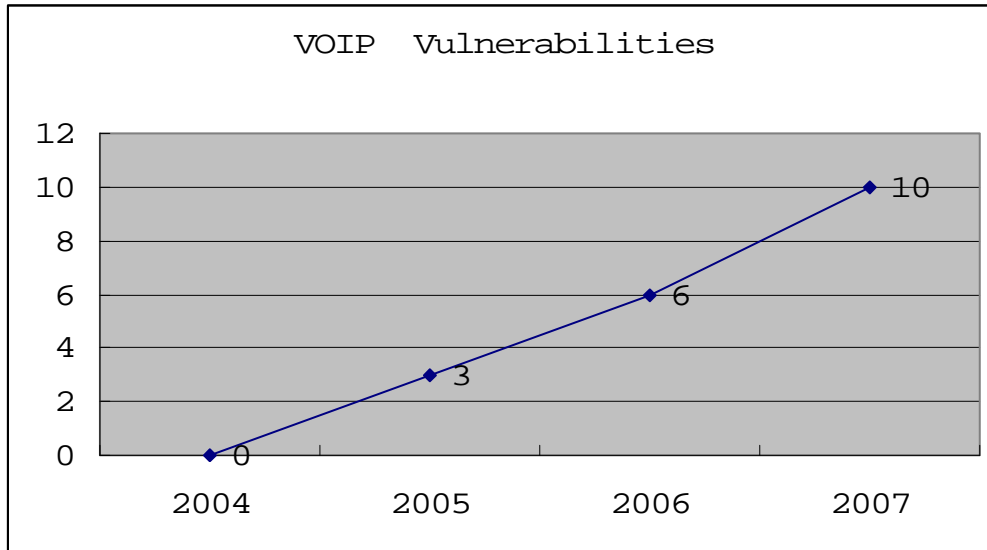
The first one has been exploited widely; one of the most famous cases being the [Windows secdrv.sys privilege escalation problem](#), which was exploited as zero-day and later reported by AV vendors.

Even though most of the SSDT hook problems were reported as Denial of Service attacks, we believe that with enough research, they might be able to be turned into Local Root.



9 VOIP

The rapid growth in use of VOIP has also caught the attention of hacker communities. The following chart explains everything:



Source: Quick search from the [Secunia](#) database

10 Mobile

With more and more people using Mobile devices, the industry is paying increasing attention to mobile security. Leading vendors have released their own solutions for mobile security.

However, according to a research firm's report, *"73 per cent of mobile users admitted they are not always cognizant of security threats and best practices. More than 25 per cent also conceded they either hardly ever or never consider security risks."*

If the users do not pay attention to, the attackers will.