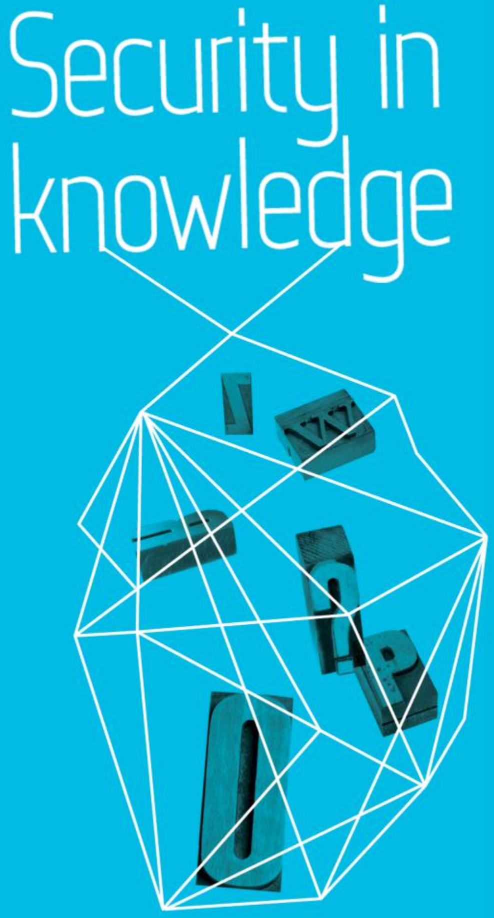
RSACONFERENCE2013

25 Years of Vulnerabilities: 1988-2012

Past, Present and Future

Yves Younan, Ph.D.
Senior Research Engineer
Sourcefire Vulnerability Research Team (VRT)



Session ID: BR-F41

Session Classification: Intermediate

Introduction

- This session will look at some vulnerability statistics
- Some of the questions we will aim to answer:
  - What are the most popular vulnerabilities?
  - Which had the most impact?
  - Which vendors and products suffered from the most issues?
  - Which browser is the best in terms of vulnerabilities found?
  - How many 0-days are found in products?

Overview

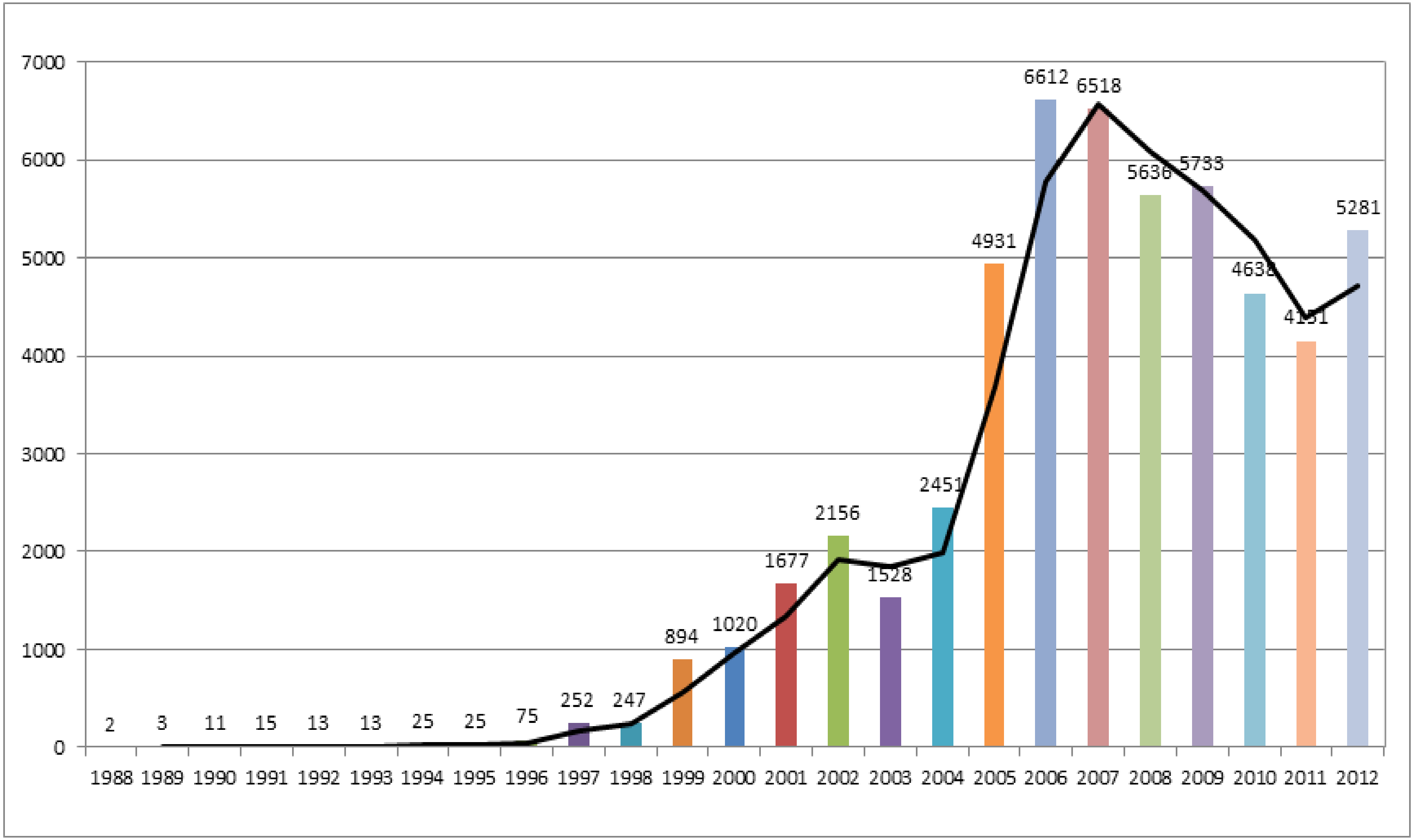
- A look at 25 years of past vulnerabilities
  - Based on the CVE/NVD data.
  - CVE started in 1999, but includes historical data going back to 1988.
  - NVD hosts all CVE information in addition to some extra data about vulnerability types, etc.
- A look at the present
  - First six weeks of 2013
- A look at the future
  - What trends do we expect?

Past

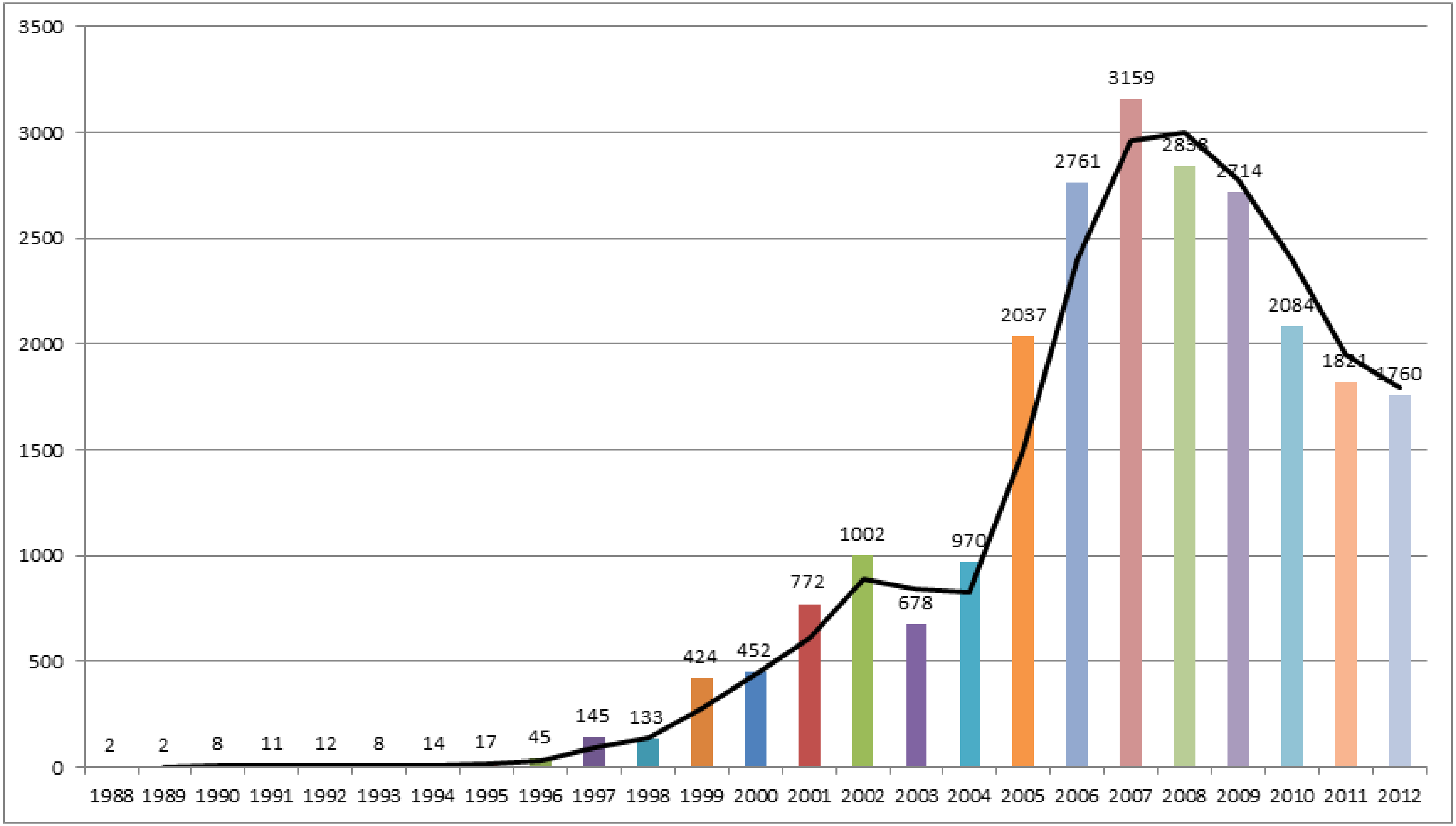
Vulnerabilities Past

- Data from 1988-2012
- More than 54,000 vulnerabilities in this period
- Majority of vulnerabilities in the last half of this period
- Common Vulnerability Scoring System (CVSS) scores for vulns gives info on seriousness of vulns
- We use the following in the stats:
  - CVSS >=7 is considered a serious vulnerability
  - CVSS = 10 is considered a critical vulnerability
    - Note: if insufficient information is available, NVD will consider the vulnerability to be critical

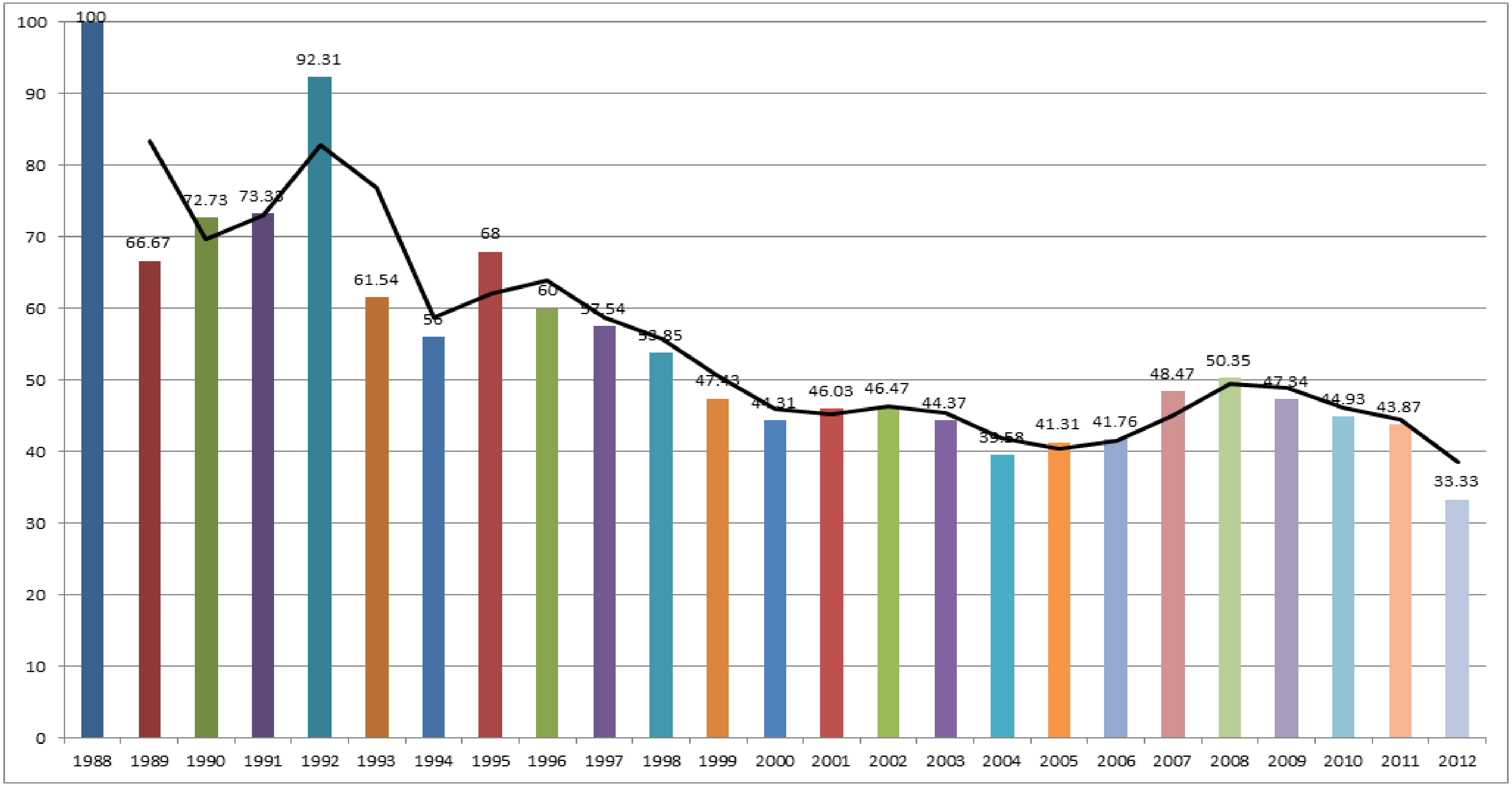
Total Vulnerabilities by Year



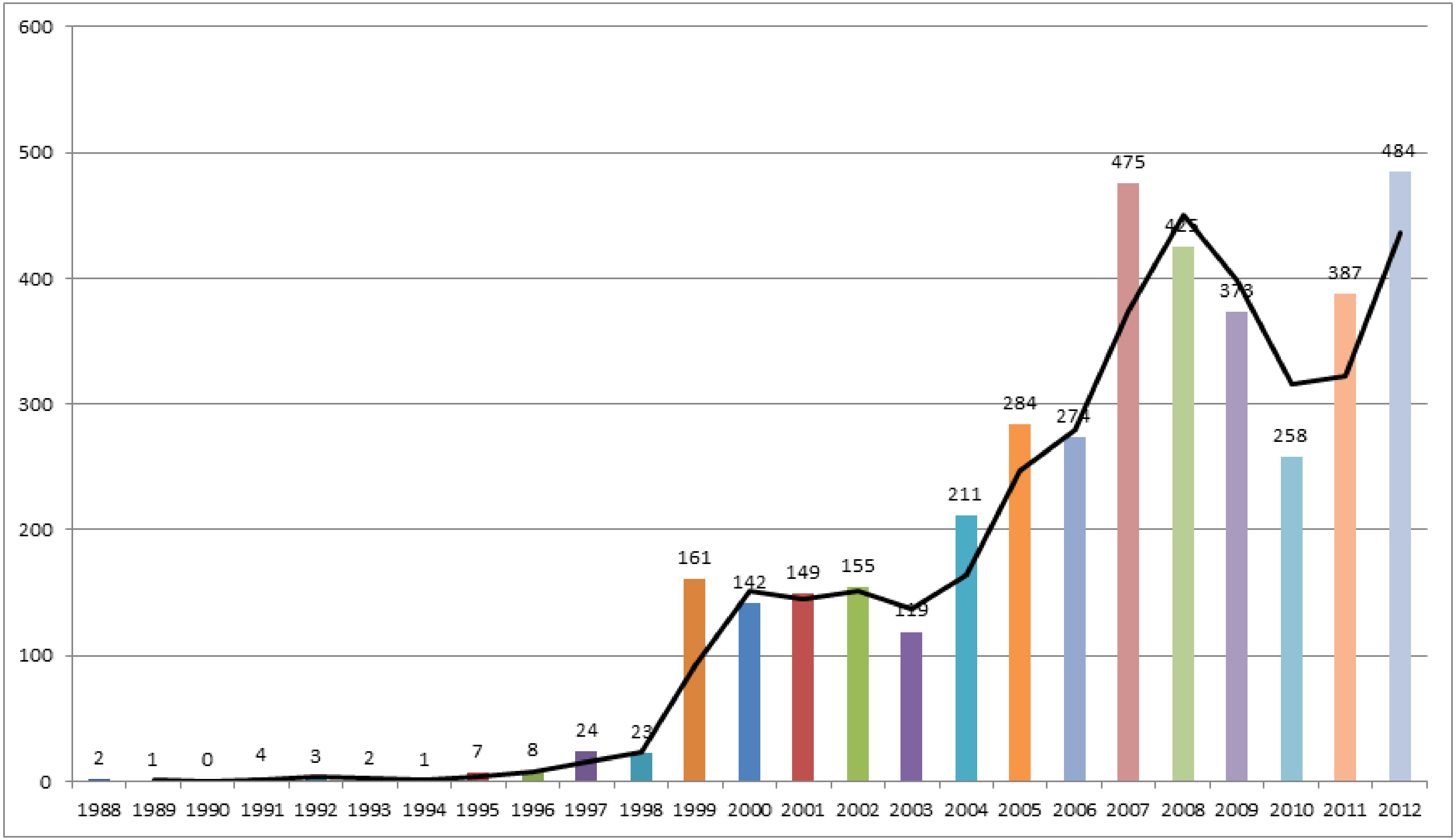
Total Serious Vulnerabilities



Serious Vulns Percentage of All Vulns



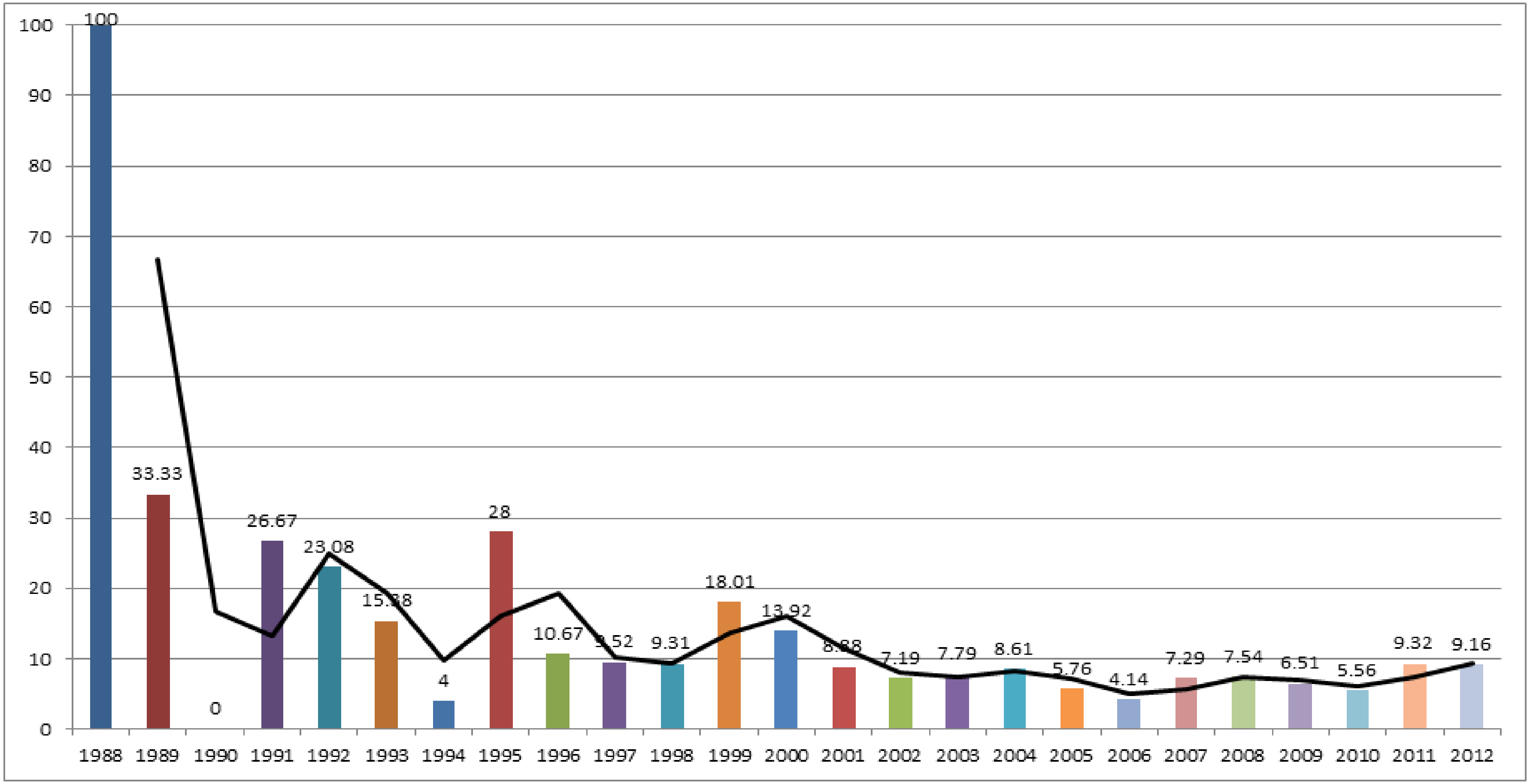
Total Critical Vulnerabilities



RSACONFERENCE2013

SOURCEfire®

Critical Vulns Percentage of All Vulns



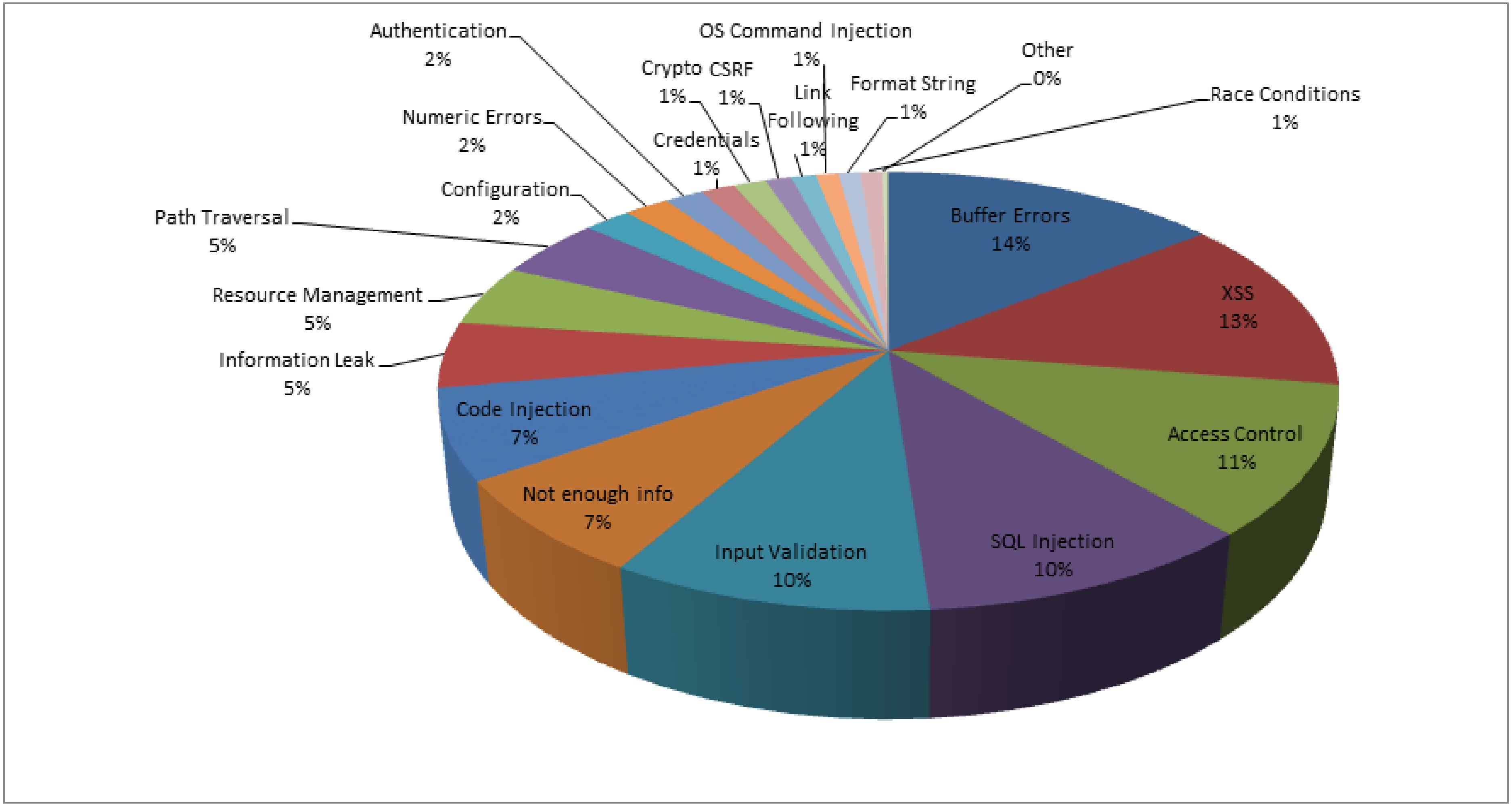
Vulnerabilities by Type

- Common Weakness Enumeration creates a number of categories for vulnerabilities
- NVD uses a subset of CWE to categorize vulnerabilities:
  - Authentication issues: not properly authenticating users
  - Credentials management: password/credential storage/transmission issues
  - Access Control: permission errors, privilege errors, etc.
  - Buffer error: buffer overflows, etc.
  - CSRF: cross-site request forgery
  - XSS: cross site scripting
  - Cryptographic issues: errors in crypto
  - Path traversal: incorrectly handling input like ".."

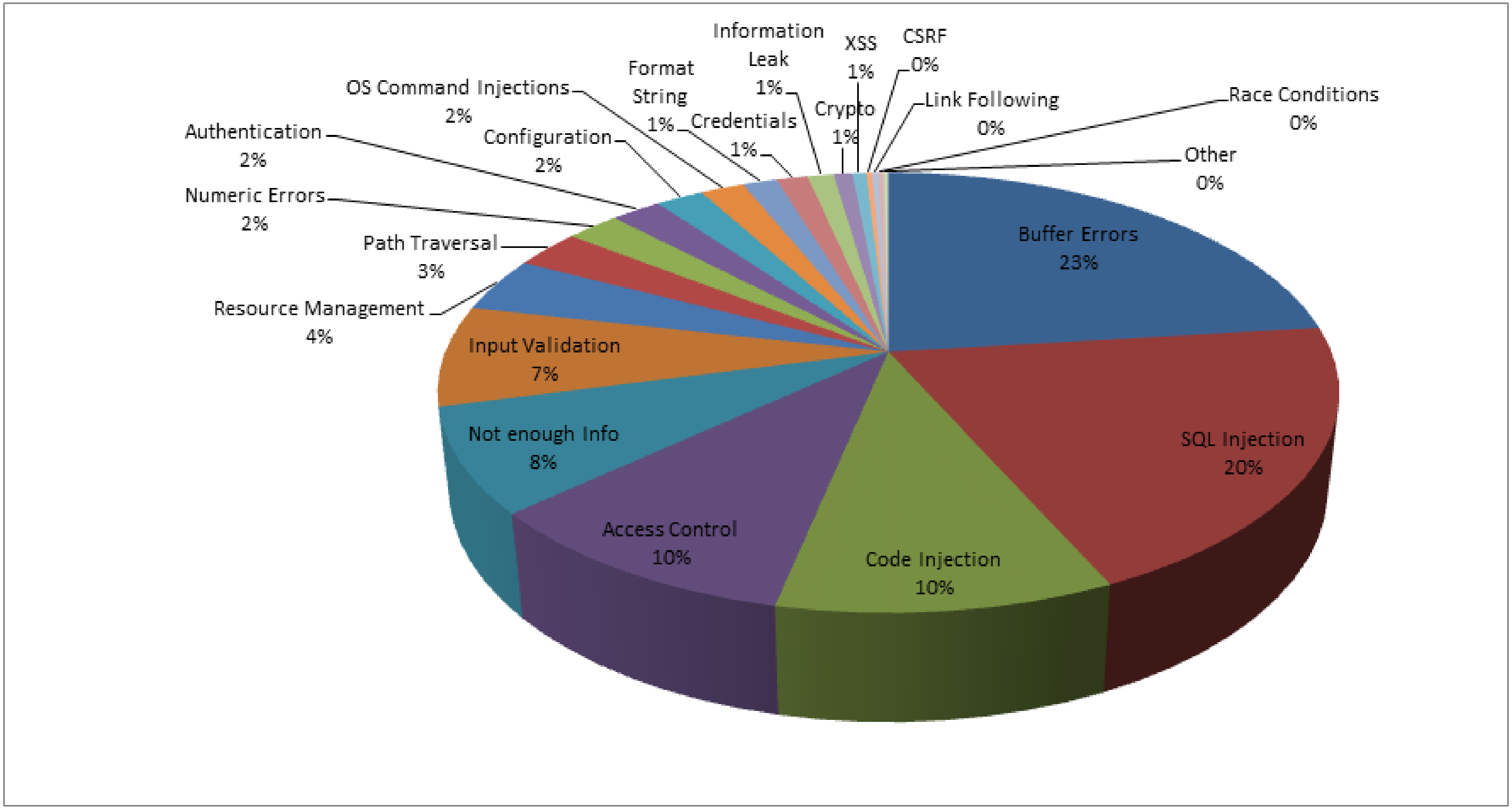
Vulnerabilities by Type

- NVD CWE subset continued:
  - Code injection: executing scripting code or similar
  - Format string vuln: attackers control specifier for formatting func.
  - Configuration: errors in configuration
  - Information leak: exposing sensitive information
  - Input validation: lack of verifying input, overlaps with others
  - Numeric errors: integer overflows, signedness errors, etc.
  - OS Command Injections: executing via command line
  - Race conditions: time of check to time of use errors
  - Resource management: memory leaks, using excess res., etc.
  - SQL injection
  - Link following: following symlinks / hard links

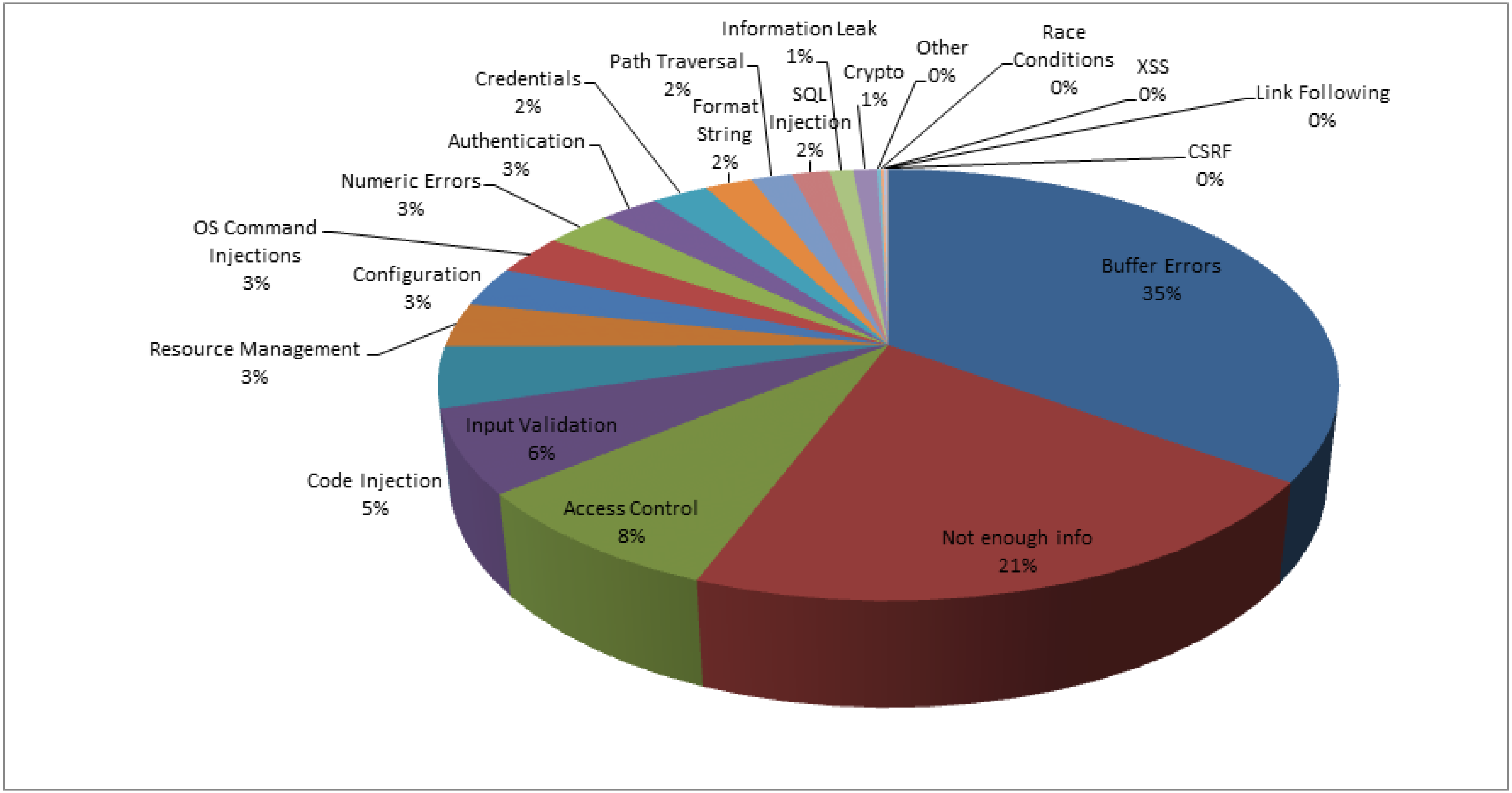
Vulnerabilities by Type



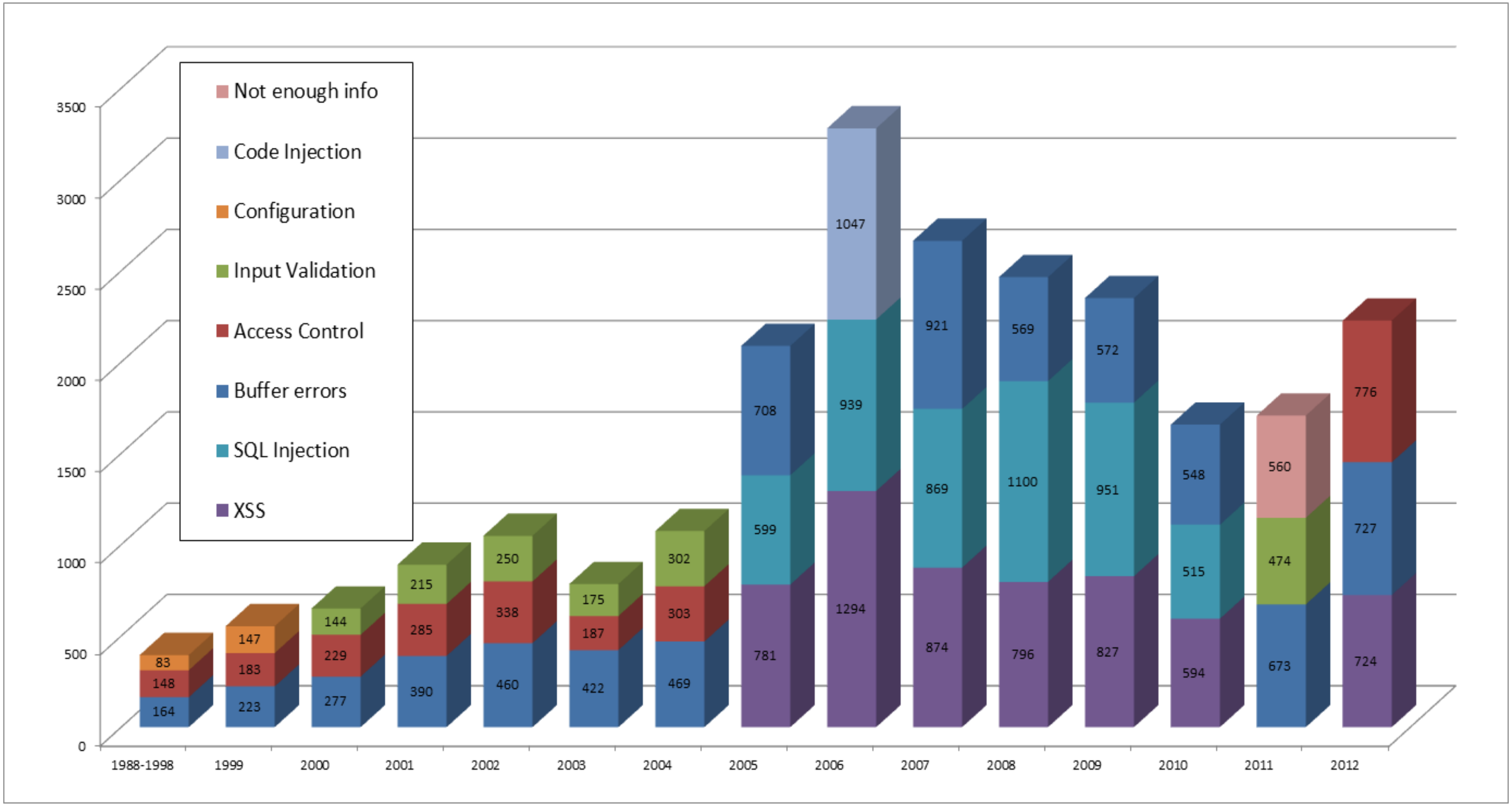
Serious Vulnerabilities by Type



Critical Vulnerabilities by Type



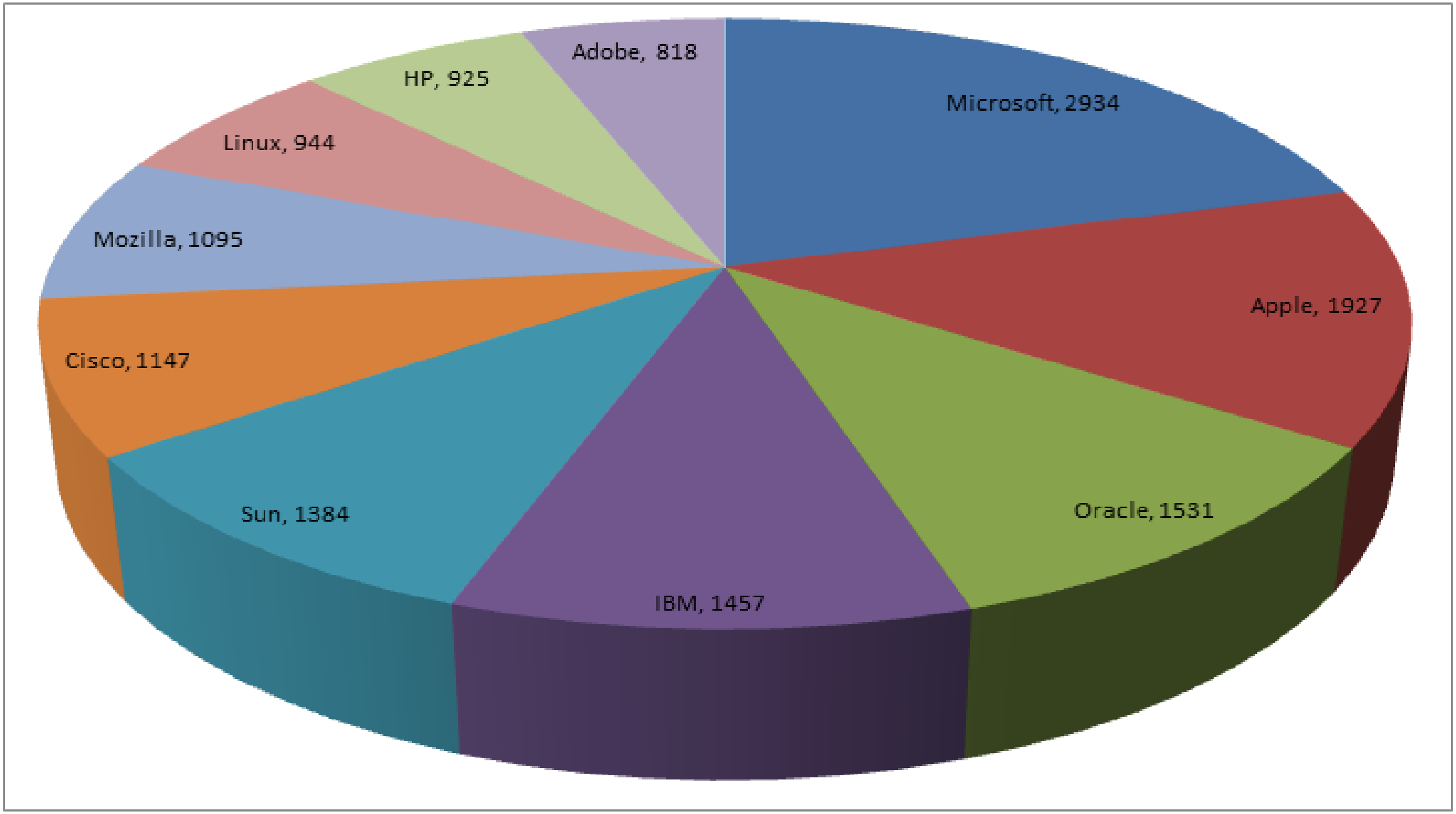
Vulnerability Types Over the Years



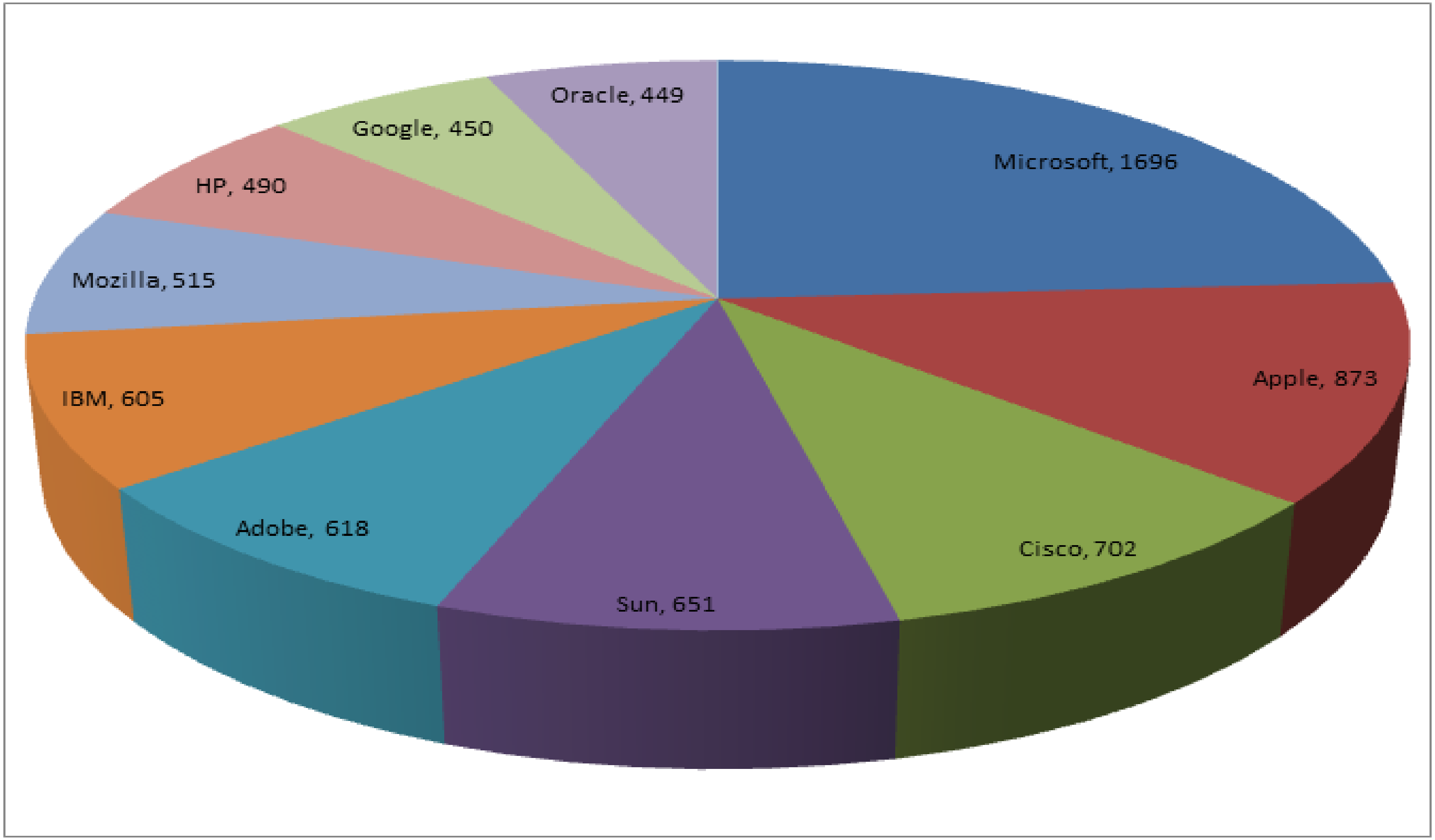
Vulnerabilities by Vendor

- NVD has information on affected product for 53,211 vulnerabilities
- Top 10 vendors account for 14,162 vulnerabilities, almost 27% of all vulnerabilities.
- Some vendors have lots of products, which can result in a higher total vulnerabilities count
- We will also look at specific products later so we can provide more extensive analysis

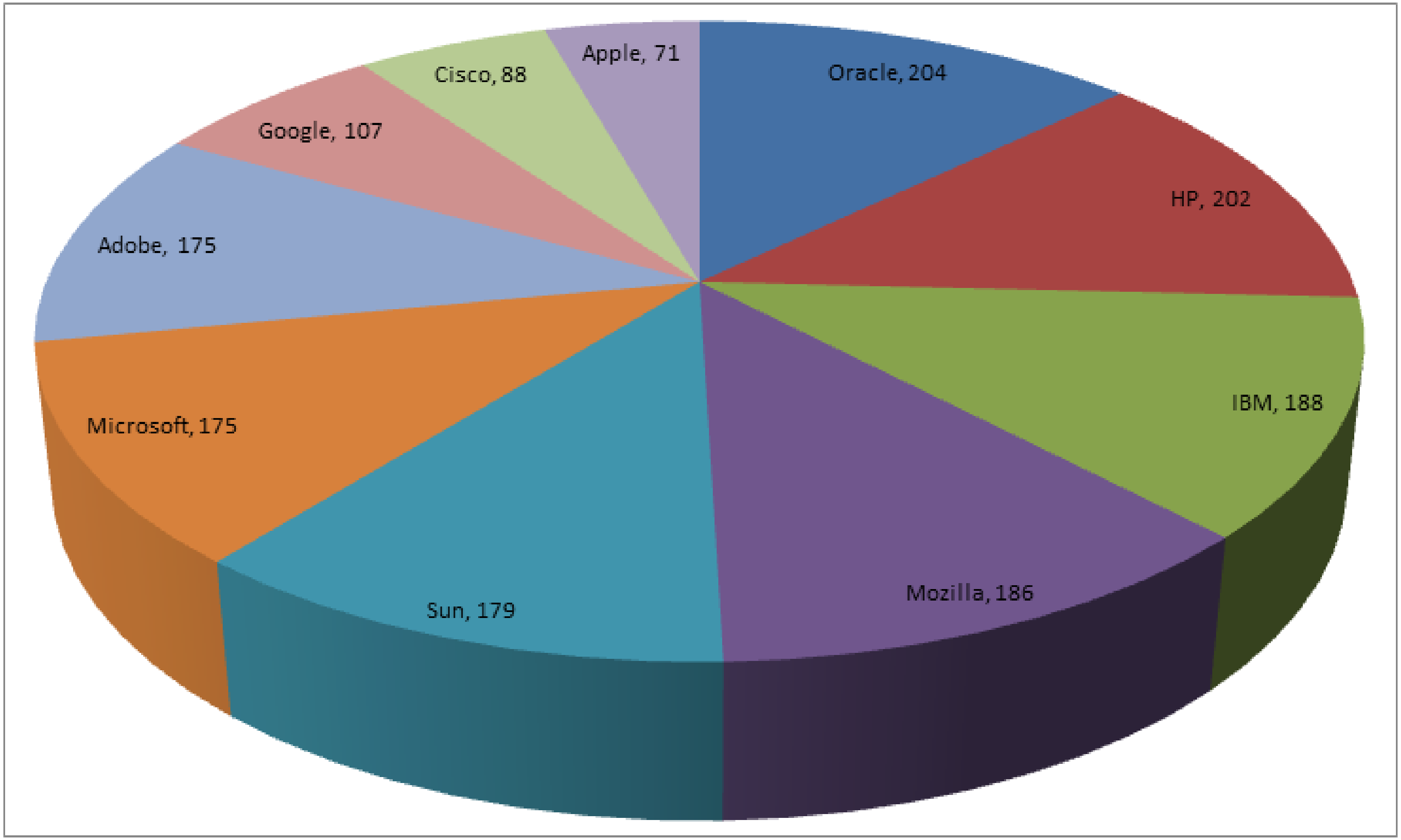
Top 10 Vendors for Total Vulns



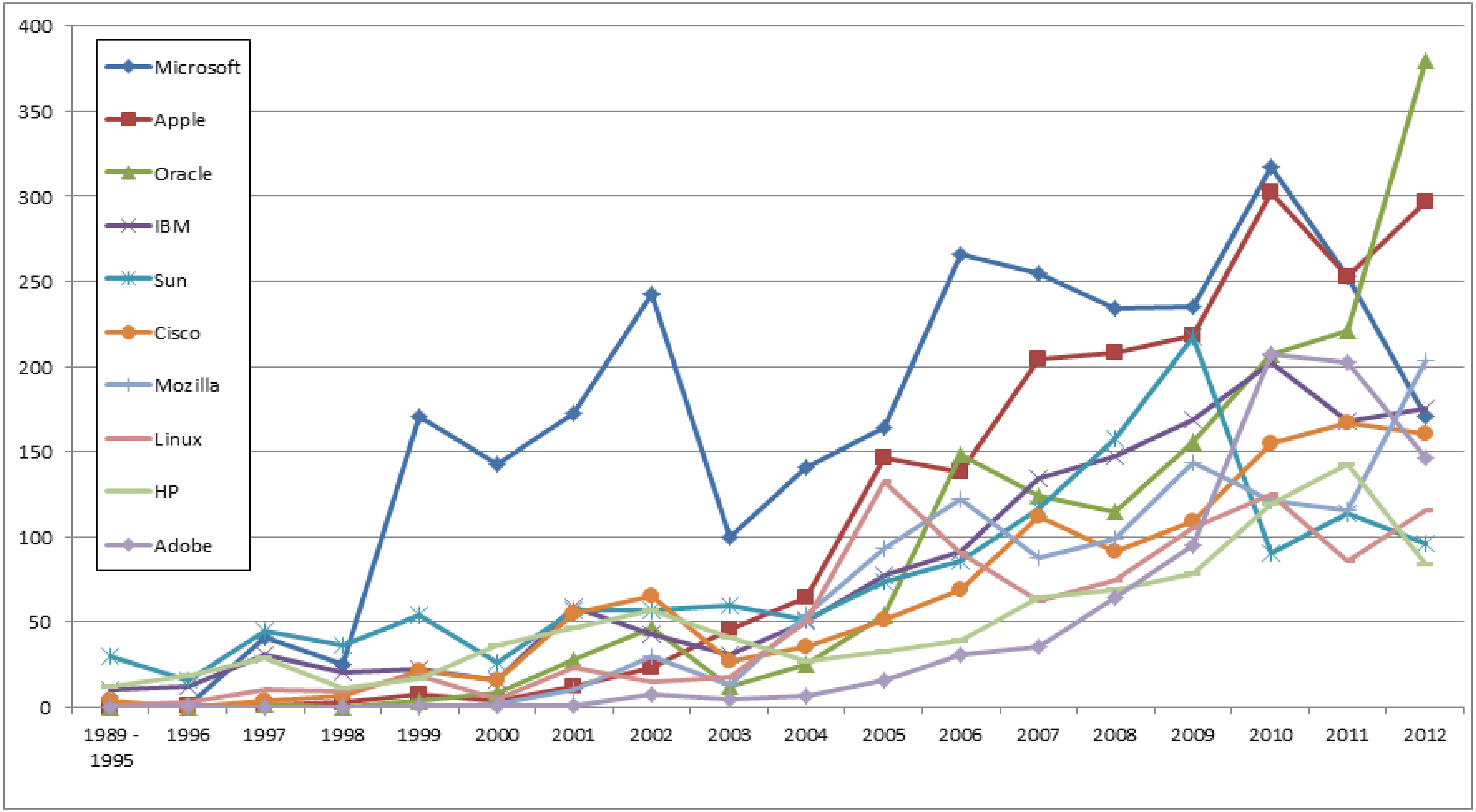
Top 10 Vendors for Serious Vulns



Top 10 Vendors for Critical Vulns



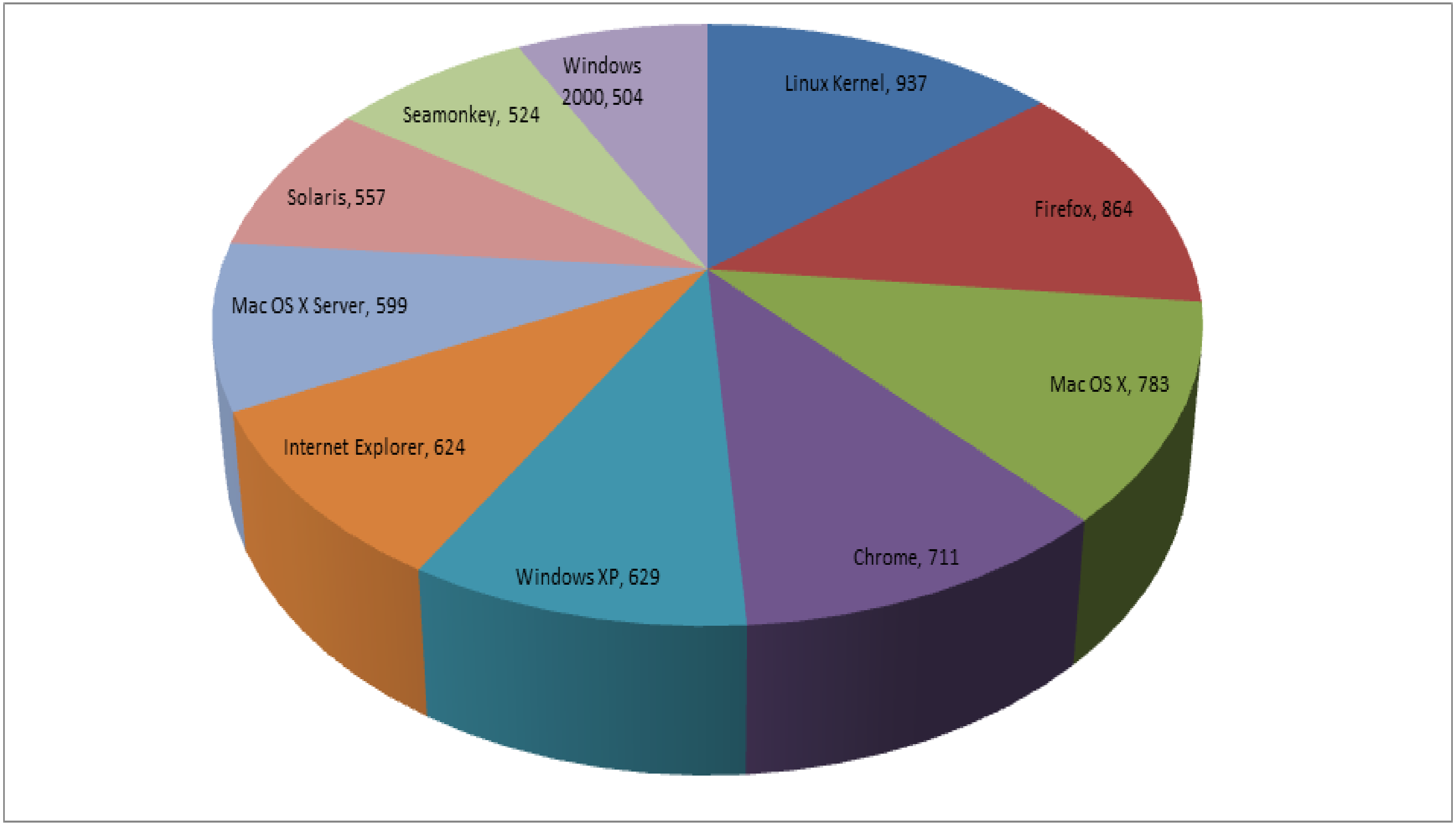
Top 10 Vendors over the Years



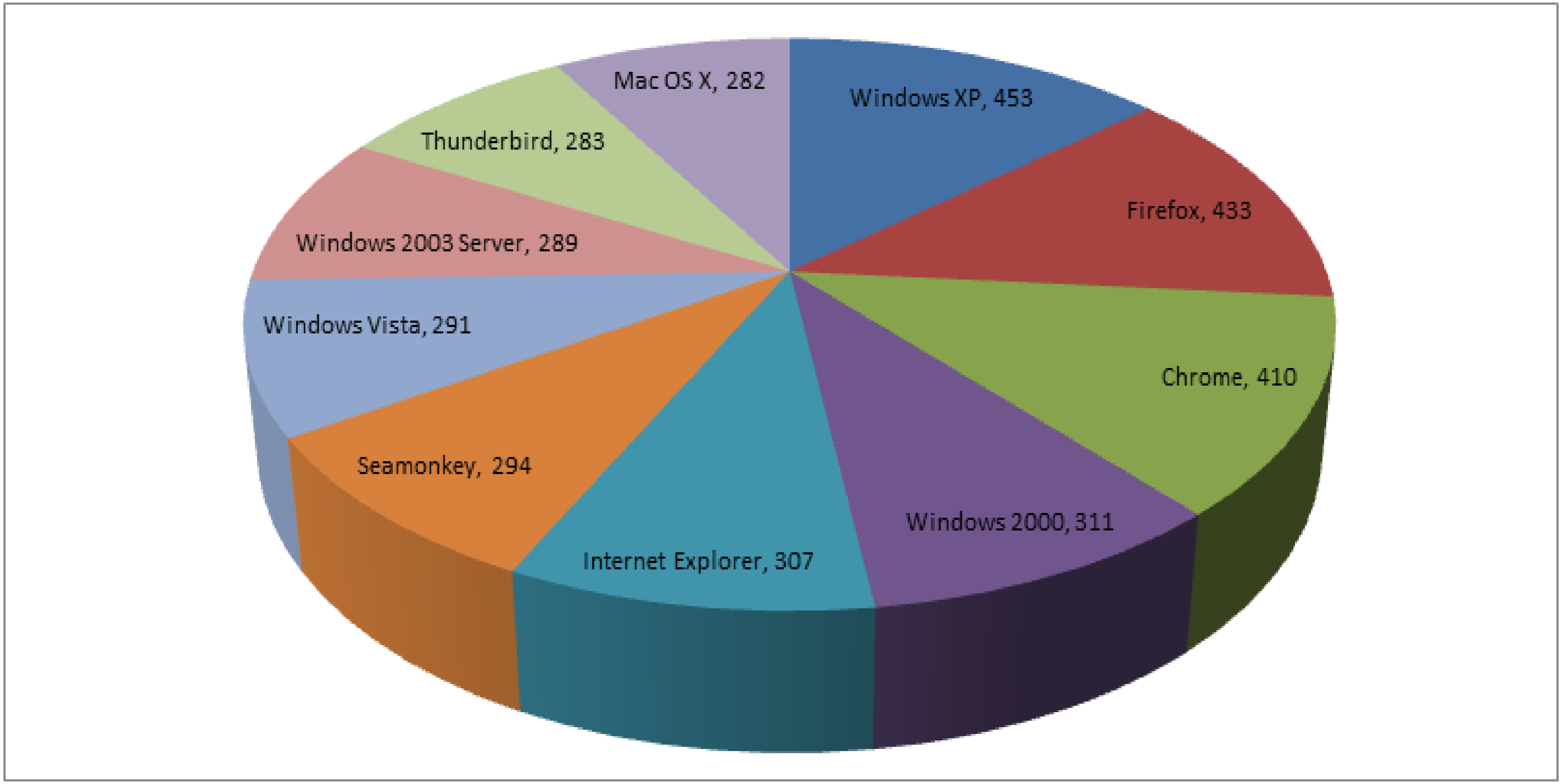
Vulnerabilities by Product

- Our vendor comparison gave us an idea who had to deal with the most vulnerabilities
- However, vendors have multiple products: having more products, will usually result in suffering from more vulnerabilities
- Here we look at product specific comparisons

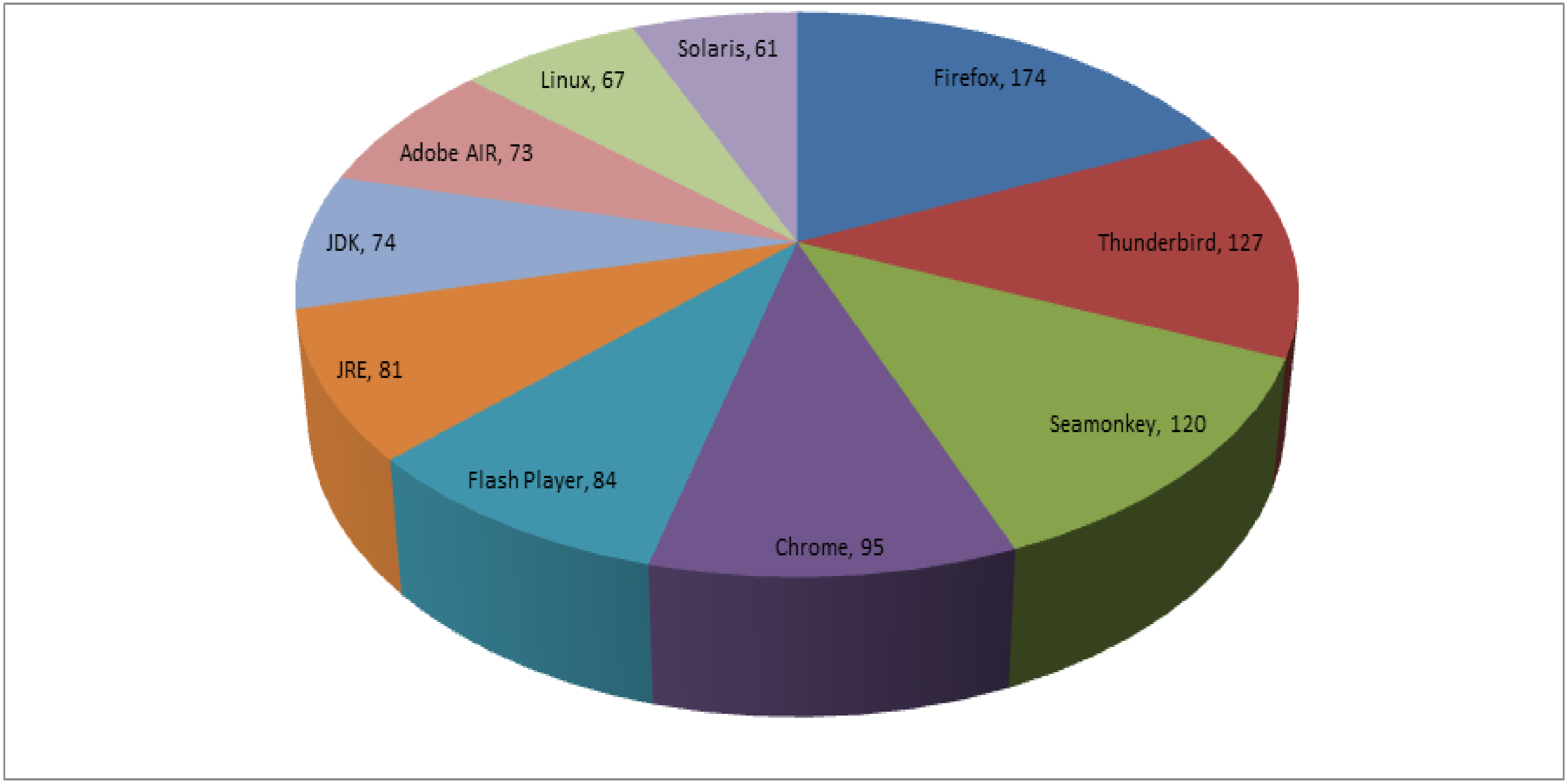
Top 10 Vulnerable Products



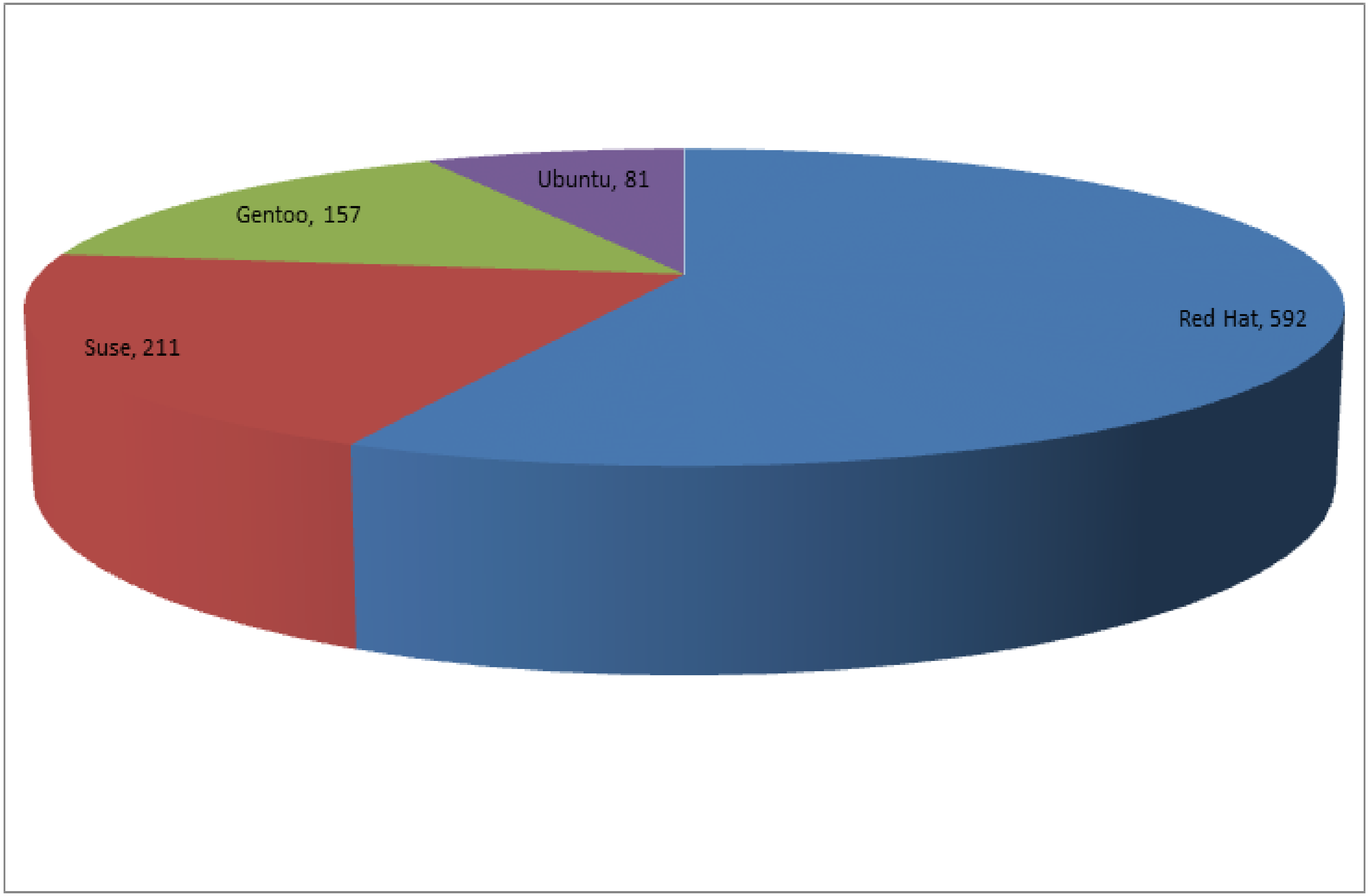
Top 10 Seriously Vulnerable Products



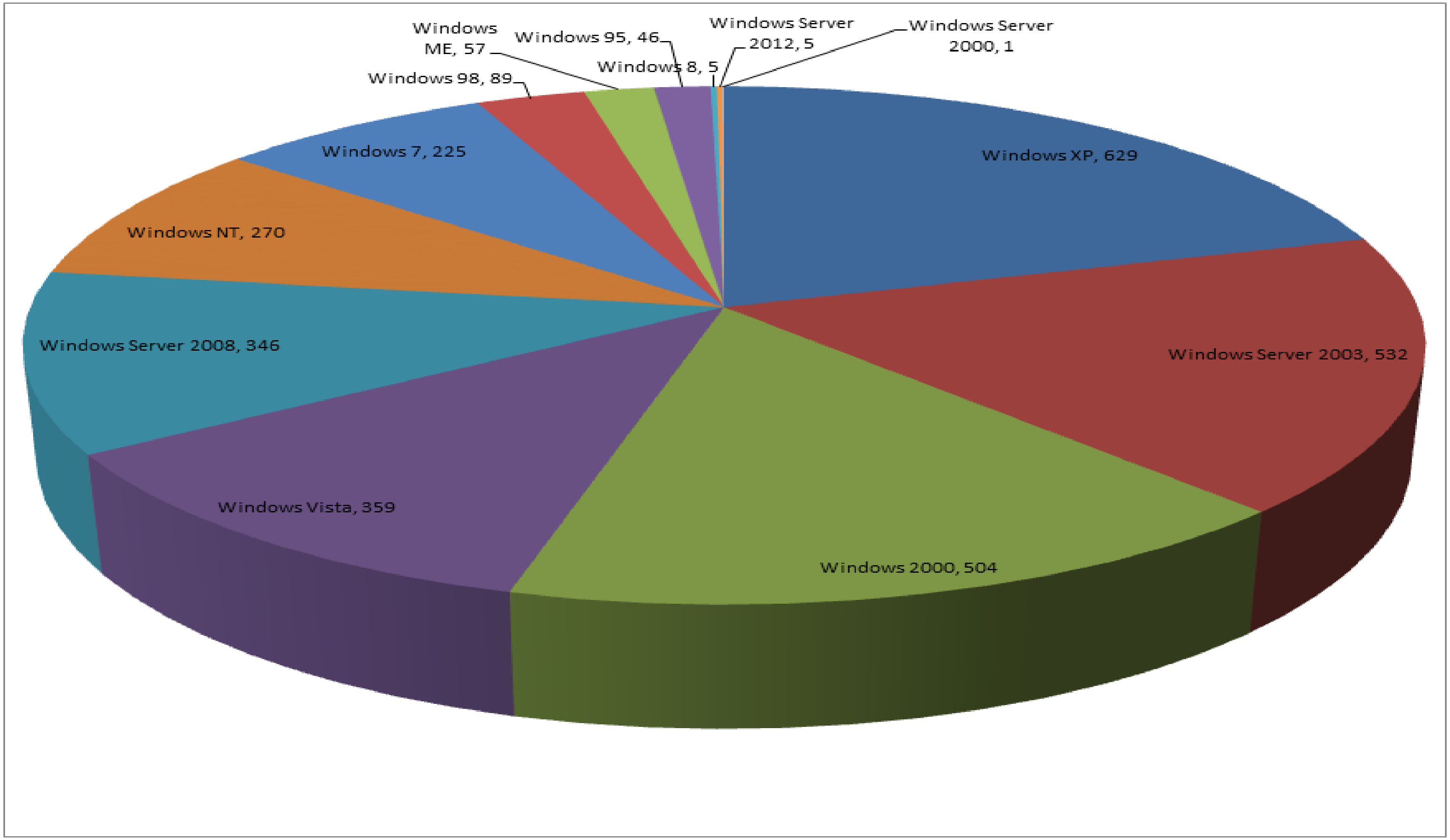
Top 10 Critically Vulnerable Products



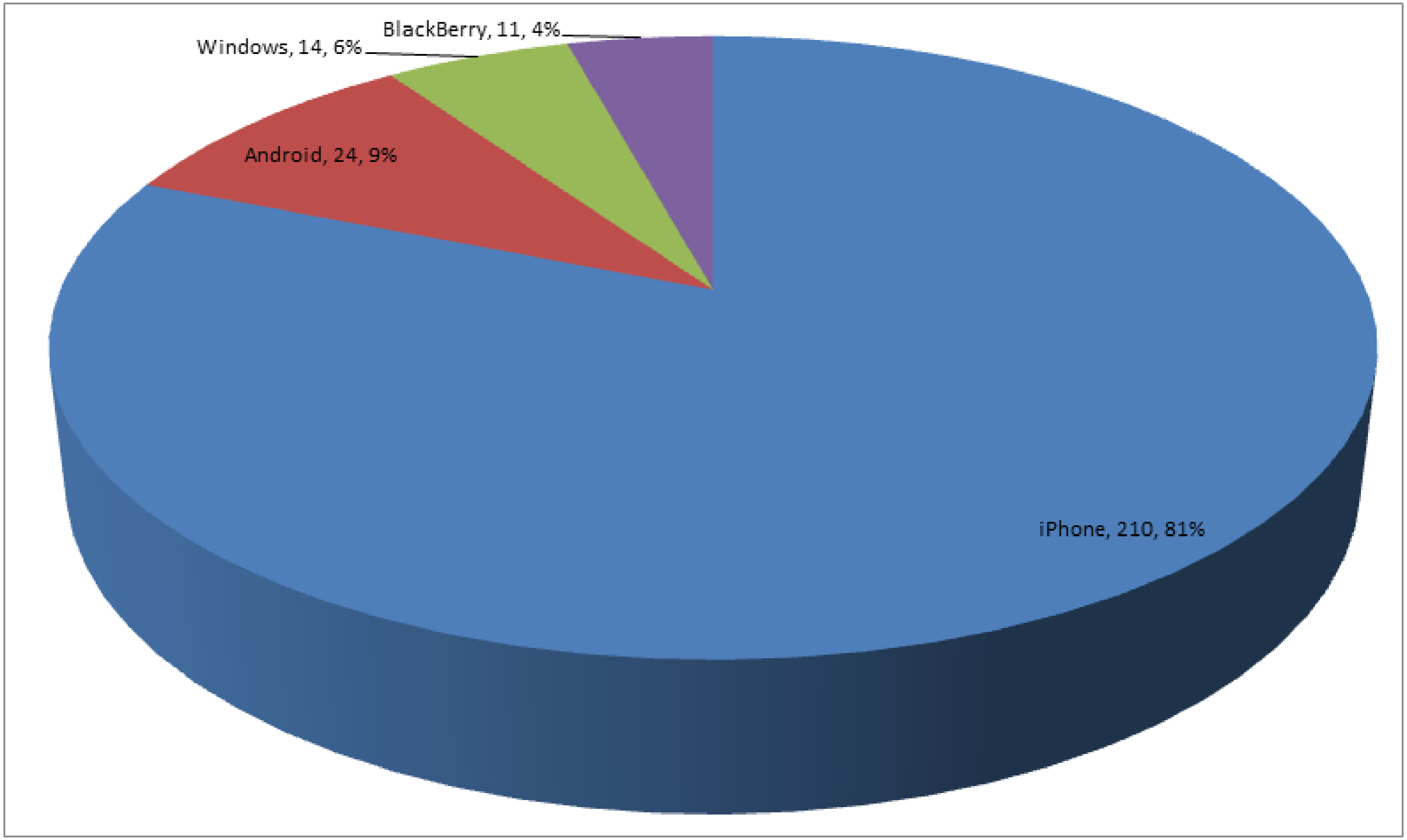
Vulnerabilities by Linux Distribution



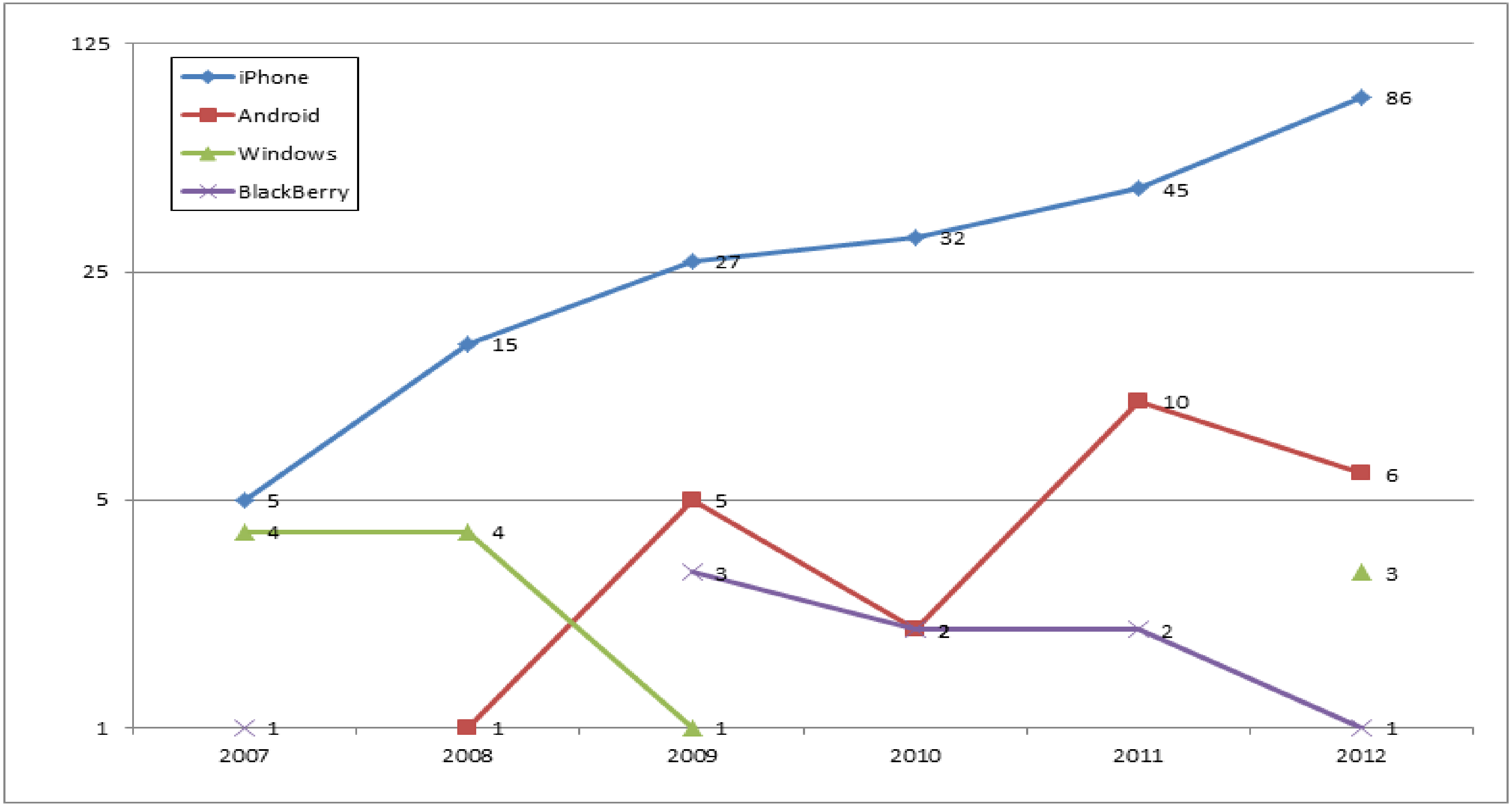
Vulnerabilities by Windows Version



Vulnerabilities by Mobile OS



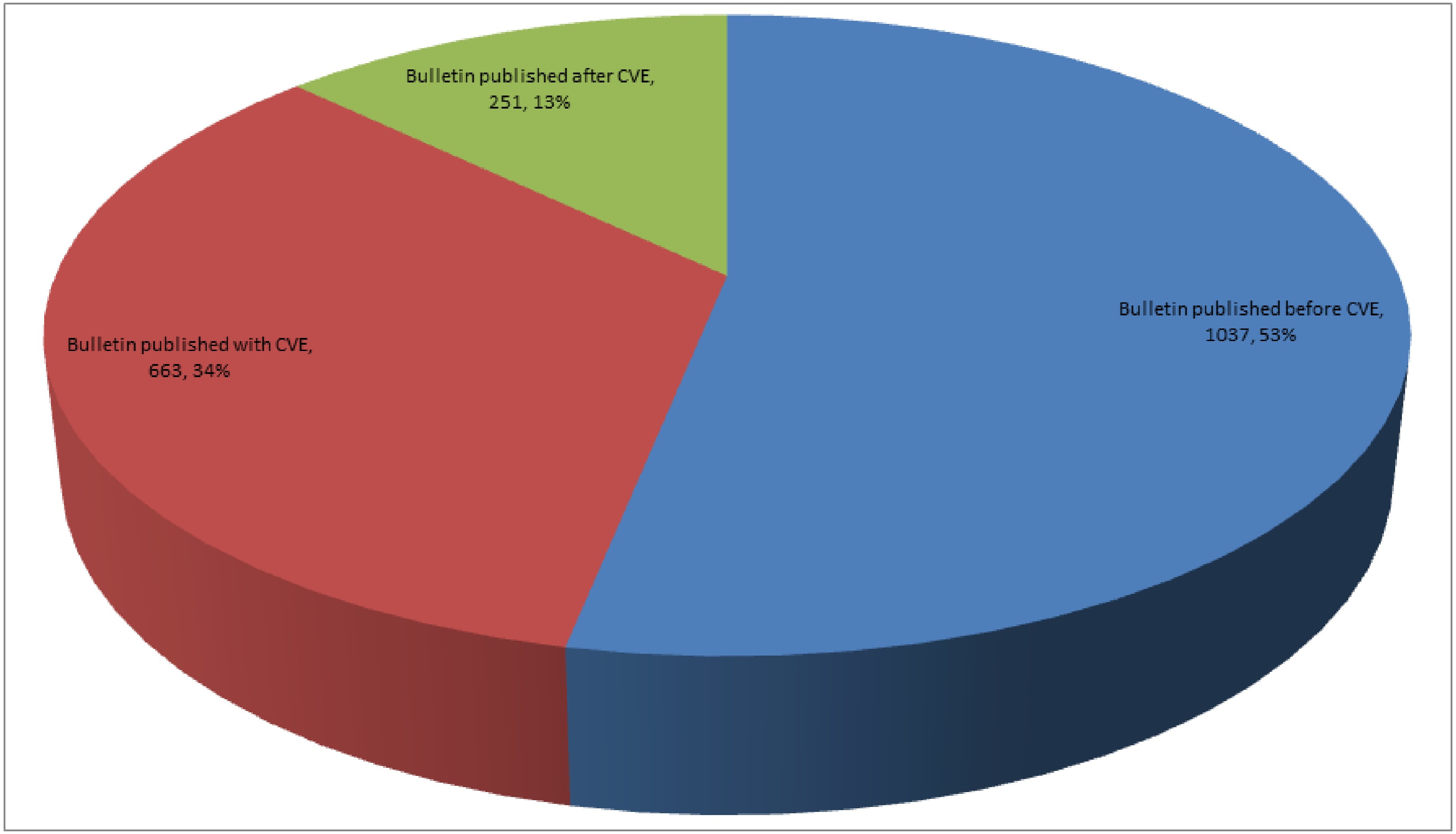
Trends in Mobile Phone Vulns



Microsoft Bulletins

- Contain information on all Microsoft vulnerabilities and associated CVEs
- Correlate the release dates of the bulletins with the release dates of the CVEs
- Gives us insight into how often vulnerabilities are 0 day vulns
  - If CVE is published before MS bulletin meaning that vulnerability information was available before a response from MS

CVE Correlated with MS Bulletins

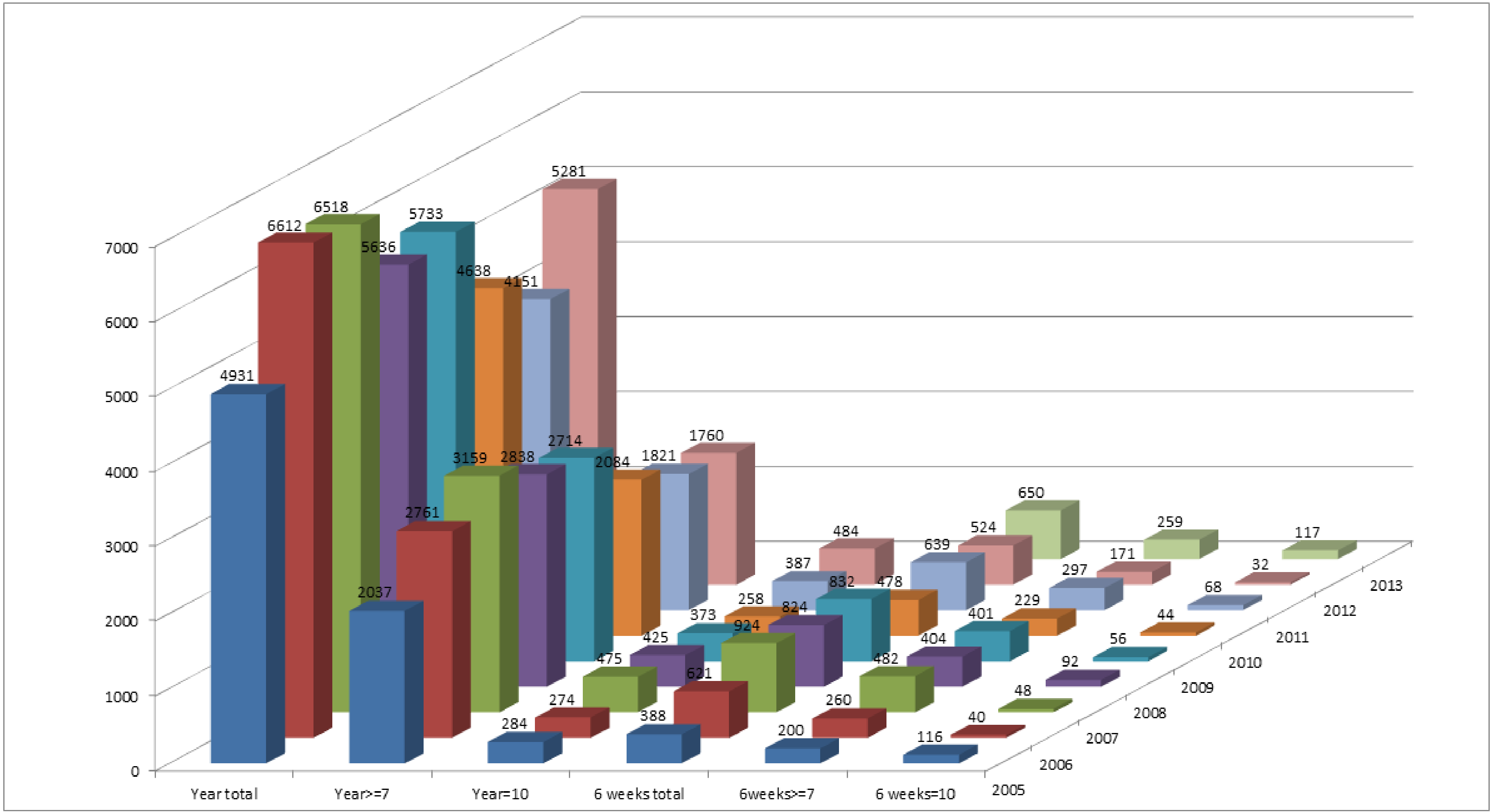


Present

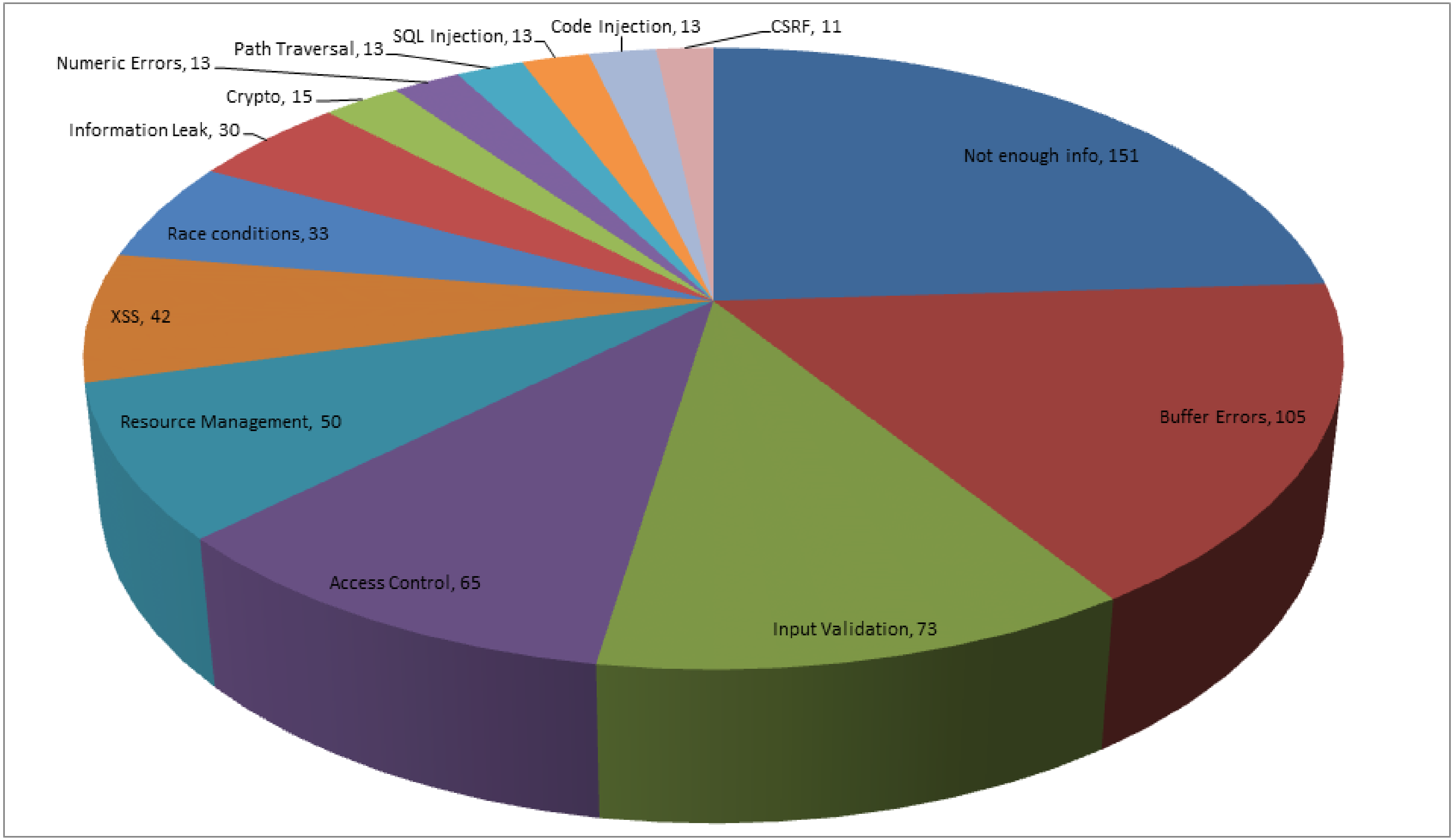
Vulnerabilities Present

- Let's take a look at the first 6 weeks of 2013: January 1st until February 14th
- We will look at total vulnerabilities this year and severity
- We will also look at the top 10 vendor and top 10 products for these first 6 weeks

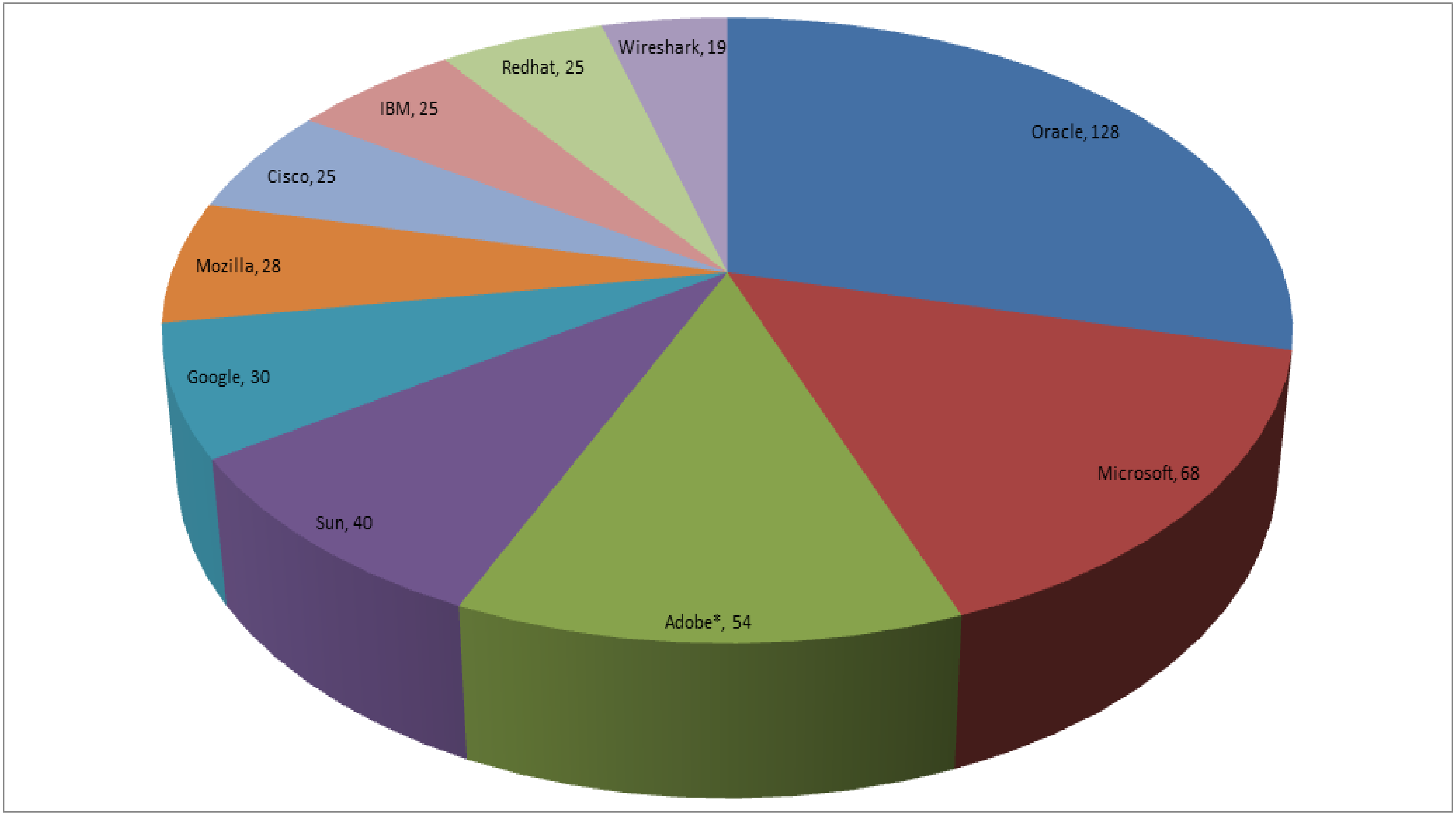
Total vulnerabilities 2013



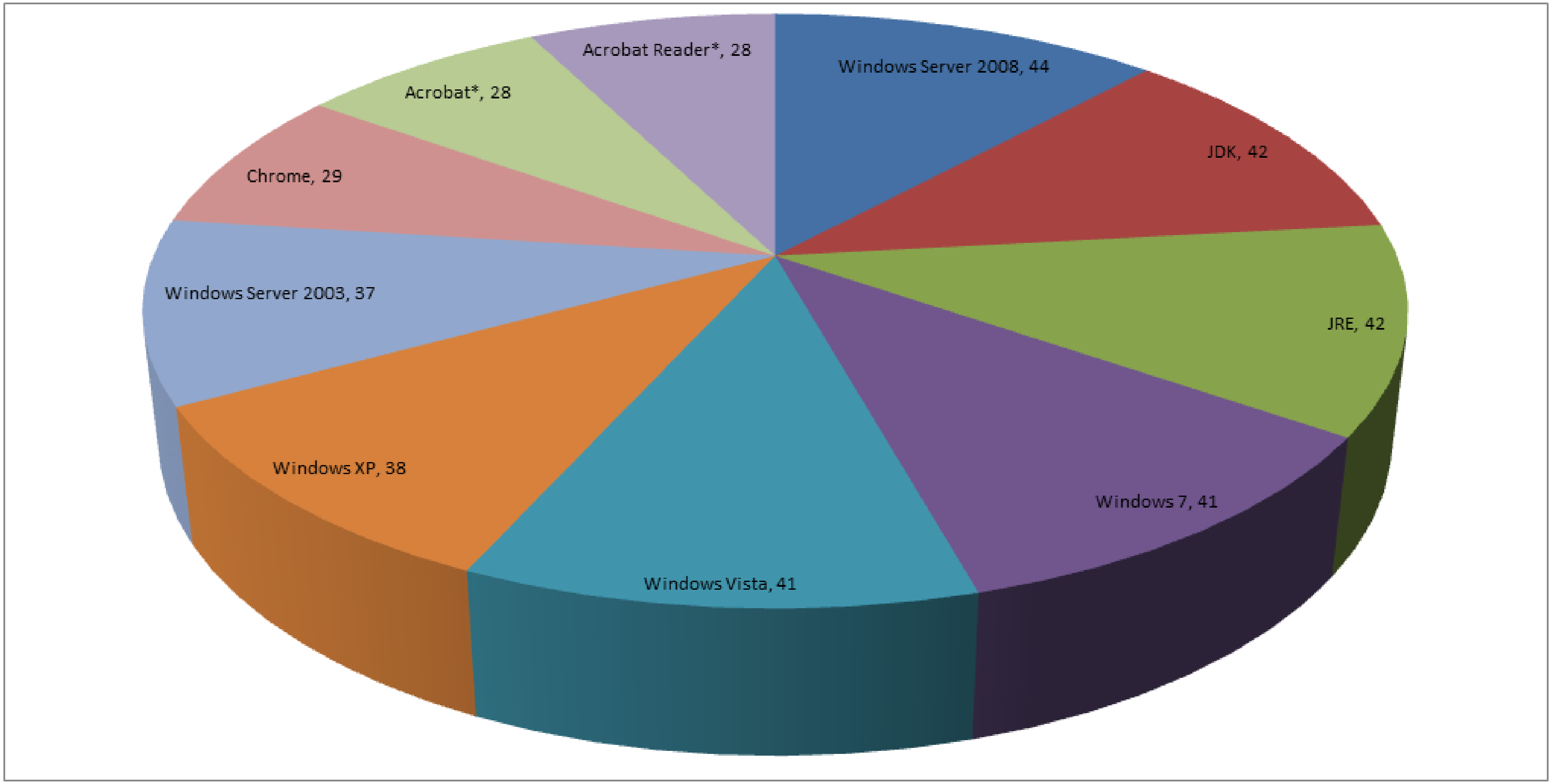
Vulnerability types 2013



Top 10 Vendors 2013



Top 10 Products 2013



Future

Vulnerabilities Future

- Plenty of static analysis tools, mitigations, etc. yet buffer overflows remain a very important vulnerability now and will probably will in the future too
- Access control / privilege issues will continue to remain important in large part due to better privilege separation
- Oracle will probably remain at the top for a while
- Google will probably enter the top 10 this year and will remain there for the foreseeable future

Conclusions

Conclusions

- Fewer vulnerabilities were reported in 2012, but the percentage of critical vulnerabilities has increased in the last 2 years
    - The trend of more critical vulnerabilities seems to be continuing into 2013
- Microsoft has significantly improved in the last couple of years, their browser and mobile OS are better than their competitors in terms of vulnerabilities discovered

Conclusions

- Apple and Google have different track records for their browsers vs. mobile operating systems
  - Chrome is ranked one of the highest for vulnerabilities
  - Android has very few
  - Safari has the fewest vulnerabilities compared to other browsers
  - iPhone has a significant lead in vulnerabilities
- Full report will be published after the conference via the VRT blog: http://vrt-blog.snort.org

Questions

?

- Contact: yyounan@sourcefire.com
- http://www.sourcefire.com
- http://www.sourcefire.com/security-technologies/snort/vulnerability-research-team/