The National Vulnerability Database

Peter Mell

NIST

12/1/05

http://nvd.nist.gov

https://nvd.nist.gov

Overview

NVD is a comprehensive information technology vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides links to industry resources.

It is built upon the CVE standard vulnerability nomenclature and augments the standard with a search engine and reference library.

U.S. Government Vulnerability Resource Integration

US-CERT
www.us-cert.gov

NIST
National Institute of Standards and Technology
ICAT
METABASE

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

MITRE

Integrated Resources

- U.S. Government
  - CVE Entries (foundation for all integration)
    - NVD would not be possible without CVE
  - US-CERT Technical Advisories
  - US-CERT Vulnerability Notes
  - OVAL Queries
  - ICAT Vulnerability Summaries
- Commercial
  - Commercial vulnerability databases
    - e.g. Bugtraq, ISS X-Force
  - Software company security advisories
    - e.g. Microsoft, Sun, Red Hat

How is NVD different from commercial vulnerability databases?

- Mission and Mandate
  - DHS/US-CERT and thus NVD has a special mission to warn the public about vulnerabilities and protect the cyber-infrastructure
  - Helps fulfill DHS's commission outlined in the National Strategy to Secure Cyberspace
  - We will not delay vulnerability publication for "paying customers"
  - Exports all data with no licensing restrictions
  - Provides official U.S. Government information

How is NVD different from commercial vulnerability databases?

- Unique Capabilities
  - includes and integrates all U.S. Government vulnerability resources
  - strives to include all industry vulnerability databases thus creating a "meta-search engine"
  - provides a fine grained search capability
  - provides user requested vulnerability statistics (i.e., statistics engine)

How is NVD different from commercial vulnerability databases?

- Standards Support
  - is the only database built completely on the Common Vulnerabilities and Exposures (CVE) vulnerability dictionary and included within the CVE website
  - is the only provider of large quantities of Common Vulnerability Scoring System (CVSS) scores
  - is the only database supporting the Open Vulnerability Assessment Language (OVAL)

NVD Search Capability

- Enables users to search a database containing virtually all known public computer vulnerabilities
- Enables searching by a variety of vulnerability characteristics
  - vulnerability severity
  - software name and version number
  - vendor name
  - vulnerability type
  - vulnerability impact
  - related exploit range
- Enables searching for vulnerabilities that contain specified US-CERT resources (e.g OVAL queries)

NVD Search Results

- Provides direct access to whatever US-CERT vulnerability resources are available
  - US-CERT Technical Alerts
  - US-CERT Vulnerability Notes
  - OVAL Queries
- Always provides access to a US-CERT NVD Vulnerability Summary

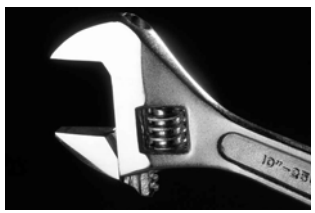
NVD Vulnerability Summaries

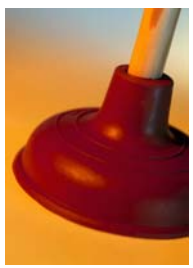
- Provides vulnerability characteristics and references
  - Description
  - Vulnerability attributes (.e.g, severity rating, related exploit range)
  - Vulnerable software and version numbers
  - Hyperlinks to US-CERT and industry resources
- Augments US-CERT existing vulnerability publications
  - ≈ 500 US-CERT Technical Alerts and CERT/CC Advisories
  - ≈ 1500 US-CERT Vulnerability Notes
  - ≈ 14000 US-CERT NVD Vulnerability Summaries

Integration with security tools

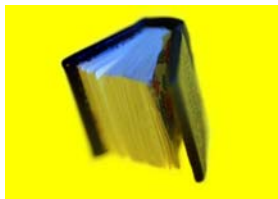
- 234 products use CVE names
- CVE vulnerability web pages map to NVD vulnerability summaries

228 CVE compatible security tools





CVE Dictionary



US Gov Advisories

Industry Advisories

Preferred

NVD Encyclopedia

CVE to NVD Integration

- NVD is a superset of the CVE dictionary
- NVD is the “CVE Database”
- NVD automatically updates as CVE changes
- CVE vulnerabilities appear on NVD within four minutes
- Vulnerabilities are fully analyzed within hours

NVD Export Capability

- XML Feed
  - Enables importation of NVD vulnerability information into third party products
  - Gives away the entire database
  - No licensing restrictions
- RSS Feed
  - Enables systems administrators and security operations personnel to keep updated on the latest vulnerabilities

NVD Target Audience

- Systems administrators
- IT security operations personnel
- Security tool companies and their users
- GOTS developers and their users
- IT forensics personnel
- Law enforcement
- Auditors
- Researchers
- Those without significant security resources

Uses

- View all publicly available U.S. Government vulnerability mitigation information
- Keep abreast on the latest vulnerabilities
- Learn how to mitigate vulnerabilities referenced within security products (e.g., intrusion detection systems)

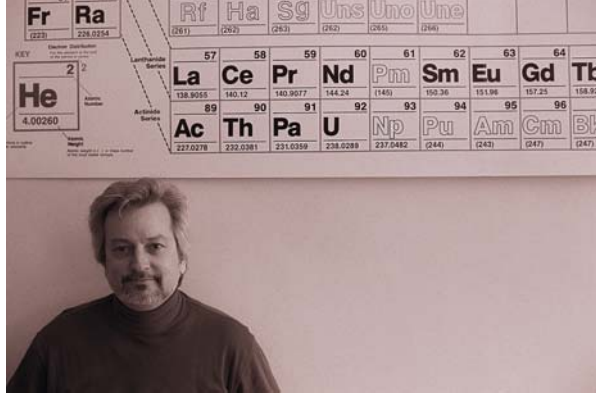
Uses

- Research the vulnerability history of a product
  - Past performance may be indicative of future performance
- Research what vulnerabilities might exist on a computer that may not be detected by vulnerability scanners (e.g., vulnerabilities in obscure products)
- View statistics on vulnerability discovery

Uses: Product Developers

- Import vulnerability information for use within their products
- Properly label a security product database with CVE names
- Properly label a security product database with OVAL names

Uses: Academia



- Vulnerability research
- Vulnerability statistics and trends

NIST Special Publication 800-51

http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf

- Contains guidance on the use of CVE within the Federal government
- Should acquire CVE compatible products
- Should monitor for CVE vulnerabilities
- Should use CVE in communicating vulnerabilities

Current Status

- Contains To Date
  - 13835 vulnerability summaries
  - 1.4 million hits per month
  - 500,000 vulnerability summaries read per month
  - Resources
    - 40 US-CERT Advisories
    - 1154 US-CERT Vulnerability Notes
    - 1012 OVAL references
    - 50,000 industry references
  - Updated every 4 minutes
  - 42 executable Cold Fusion programs

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

Resource Status

NVD contains:
13835 CVE Vulnerabilities
40 US-CERT Alerts
1154 US-CERT Vuln Notes
1012 Oval Queries
Last updated:
12/01/05
Publication rate:
17 vulnerabilities / day

Search CVE Vulnerability Database

(Perform Advanced Search)

Keyword search: Search All

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search last 3 months | Search last 3 years

Show only vulnerabilities that have the following associated resources:

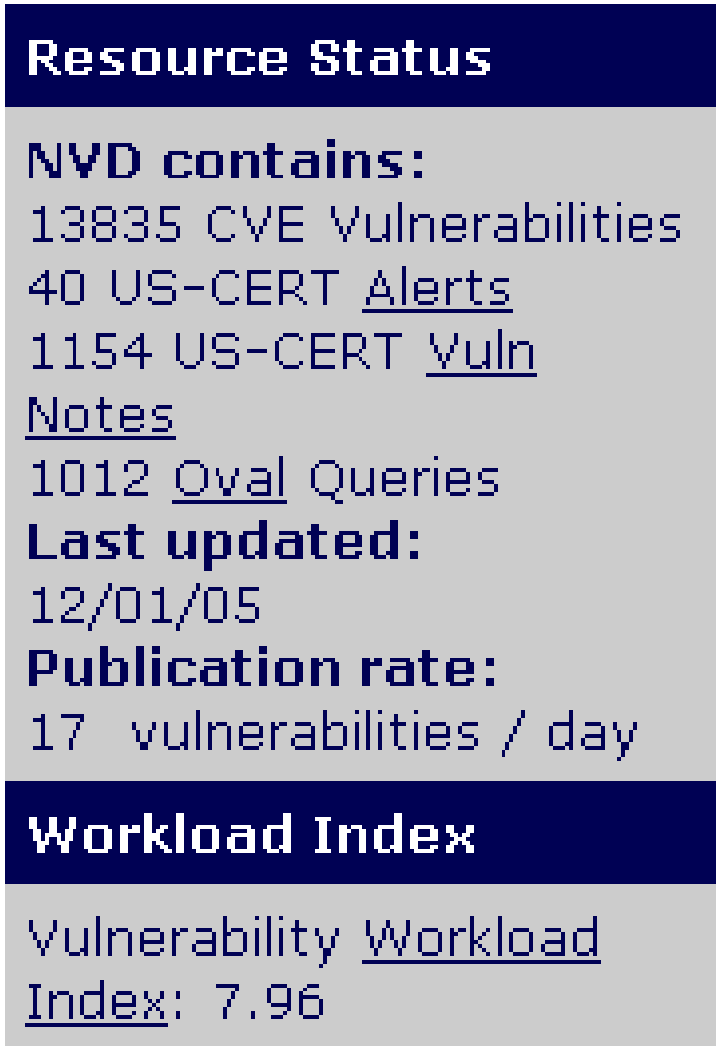
- ☐ US-CERT Technical Alerts
- ☐ US-CERT Vulnerability Notes
- ☐ OVAL Queries

Recent CVE Vulnerabilities

CVE-2005-3961 **Publish Date:** 12/1/2005
WebCalendar 1.0.1 allows remote attackers to overwrite WebCalendar data files via a modified id parameter.

CVE-2005-3960 **Publish Date:** 12/1/2005
Kadu 0.4.2 and 0.5.0pre allows remote attackers to cause a denial of service (crash or generated traffic) via a malformed message, possibly with incomplete information.

CVE-2005-3959 **Publish Date:** 12/1/2005
Multiple cross-site scripting (XSS) vulnerabilities in FreeWebStat 1.0 rev37 allow remote



The workload index can be viewed as the average number of important vulnerabilities an operations person needs to handle each day.

Equation used to calculate the workload index:

((number of high severity vulnerabilities published within the last 30 days) + (number of medium severity vulnerabilities published within the last 30 days/5) + (number of low severity vulnerabilities published within the last 30 days/20)) / 30

Advanced Vulnerability Search Page

Search Reset Values

Keyword search:

Try a vendor name, product name, or version number
Try a CVE standard vulnerability name
You can type in multiple keywords separated by spaces
Only vulnerabilities that match ALL keywords will be returned

Vendor A..B C..E F..H I..K L..N O..Q R..T U..W X..Z All

Product A..B C..E F..H I..K L..N O..Q R..T U..W X..Z All

Version ^ --- Choose a Vendor or Product --- ^

Search start date: Any Month Any Year

Search end date: Any Month Any Year

Vulnerability Severity: Any.....

Related Exploit Range: Any.....

Impact Type: Any.....

Vulnerability Type: Any.....

Show only vulnerabilities that have the following associated resources:

- US-CERT Technical Alerts
- US-CERT Vulnerability Notes
- US-CERT Technical Alerts or Vulnerability Notes
- OVAL Queries

CVE Vulnerability Database Advanced Search

Search Reset Values

Keyword search:

Try a vendor name, product name, or version number
Try a CVE standard vulnerability name
You can type in multiple keywords separated by spaces
Only vulnerabilities that match ALL keywords will be returned

Vendor	**Microsoft**
Product	IIS
Version	Any
Search start date:	Any Month / Any Year
Search end date:	Any Month / Any Year
Vulnerability Severity:	High (CVSS 7-10)
Related Exploit Range:	Remotely exploitable
Impact Type:	Any
Vulnerability Type:	Any
Show only vulnerabilities that have the following associated resources:	☐ US-CERT Technical Alerts ☐ US-CERT Vulnerability Notes ☐ OVAL Queries

There are **35** matching records. Displaying matches **1** through **20**.

Next 20 Matches

CVE-2004-0119 **TA04-104A** **VU#638548** **OVAL1997** **OVAL1962** **OVAL1808**

Summary: The Negotiate Security Software Provider (SSP) interface in Windows 2000, Windows XP, and Windows Server 2003, allows remote attackers to cause a denial of service (crash from null dereference) or execute arbitrary code via a crafted SPNEGO NegTokenInit request during authentication protocol selection.
Published: 6/1/2004
CVSS Severity: 8 (High) Approximated

CVE-2003-0224 **OVAL483**

Summary: Buffer overflow in ssinc.dll for Microsoft Internet Information Services (IIS) 5.0 allows local users to execute arbitrary code via a web page with a Server Side Include (SSI) directive with a long filename, aka "Server Side Include Web Pages Buffer Overrun."
Published: 6/9/2003
CVSS Severity: 10 (High) Approximated

CVE-2003-0223 **OVAL66**

Summary: Cross-site scripting vulnerability (XSS) in the ASP function responsible for redirection in Microsoft Internet Information Server (IIS) 4.0, 5.0, and 5.1 allows remote attackers to embed a URL containing script in a redirection message.
Published: 6/9/2003
CVSS Severity: 10 (High) Approximated

CVE-2002-1700

Summary: Cross-site scripting vulnerability (XSS) in the missing template handler in Macromedia ColdFusion MX allows remote attackers to execute arbitrary script as other users by injecting script into the HTTP request for the name of a template, which is not filtered in the resulting 404 error message.
Published: 12/31/2002
CVSS Severity: 8 (High) Approximated

National Cyber-Alert System

Vulnerability Summary CVE-2005-1208

Original release date: 6/14/2005
Last revised: 10/20/2005
Source: US-CERT/NIST

Overview

Integer overflow in Microsoft Windows 98, 2000, XP SP2 and earlier, and Server 2003 SP1 and earlier allows remote attackers to execute arbitrary code via a crafted compiled Help (.CHM) file with a large size field that triggers a heap-based buffer overflow, as demonstrated using a "ms-its:" URL in Internet Explorer.

Impact

CVSS Severity: 10 (High) Approximated
Range: Remotely exploitable
Impact Type: Provides administrator access

References to Advisories, Solutions, and Tools

US-CERT Technical Alert: TA05-165A
Name: TA05-165A
Type: Advisory , **Patch Information**
Hyperlink: http://www.us-cert.gov/cas/techalerts/TA05-165A.html

US-CERT Vulnerability Note: VU#851869
Name: VU#851869
Type: Advisory , **Patch Information**
Hyperlink: http://www.kb.cert.org/vuls/id/851869

Vulnerable software and versions

Microsoft, Windows 2000
Microsoft, Windows 98
Microsoft, Windows XP, Tablet PC Edition SP2
Microsoft, Windows XP, Tablet PC Edition SP1
Microsoft, Windows XP, Tablet PC Edition
Microsoft, Windows XP, SP2
Microsoft, Windows XP, SP1
Microsoft, Windows XP, Professional SP2
Microsoft, Windows XP, Professional SP1
Microsoft, Windows XP, Professional 64-bit
Microsoft, Windows XP, Professional
Microsoft, Windows XP, Media Center Edition SP2
Microsoft, Windows XP, Media Center Edition SP1
Microsoft, Windows XP, Media Center Edition
Microsoft, Windows XP, Home SP2
Microsoft, Windows XP, Home SP1
Microsoft, Windows XP, Home
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,
Microsoft,

Technical Details

CVSS Base Score Descriptor: (AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N) Approximated

Vulnerability Type: Buffer Overflow

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1208

Statistics Query Page

This is a general purpose vulnerability statistics generation engine. Use it to graph and chart vulnerabilities discovered within a product or to graph and chart sets of vulnerabilities containing particular characteristics (e.g. remotely exploitable buffer overflows). These calculations may take up to several minutes to be generated depending on the complexity of the statistic requested.

Vendor A..B C..E F..H I..K L..N O..Q R..T U..W X..Z All

Product A..B C..E F..H I..K L..N O..Q R..T U..W X..Z All

Version ^ --- Choose a Vendor or Product --- ^

Search start date: Any Month Any Year

Search end date: Any Month Any Year

Vulnerability Severity: Any.....

Associated Exploit Range: Any.....

Impact Type: Any.....

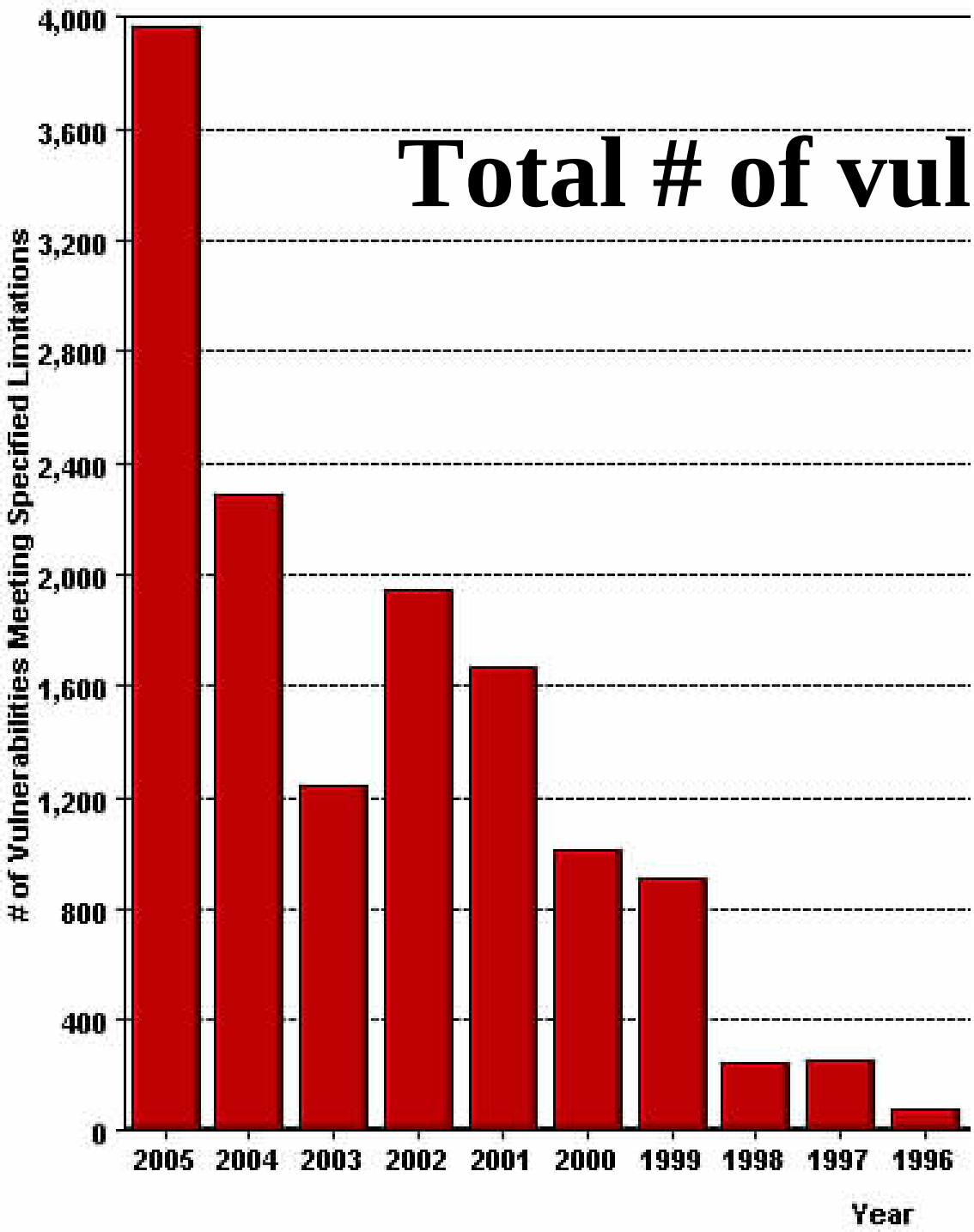
Vulnerability Type: Any.....

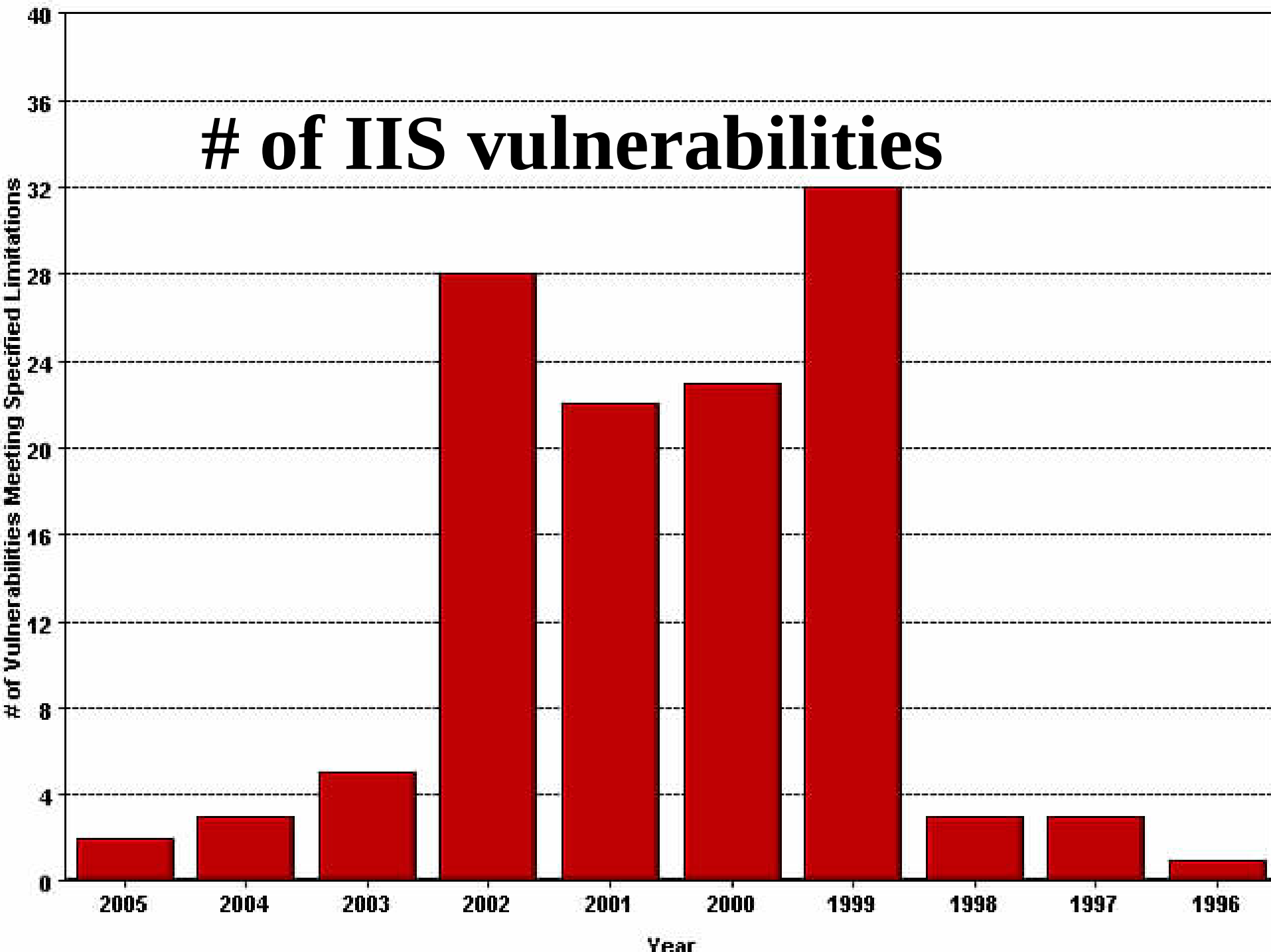
Use only vulnerabilities that have the following associated resources:

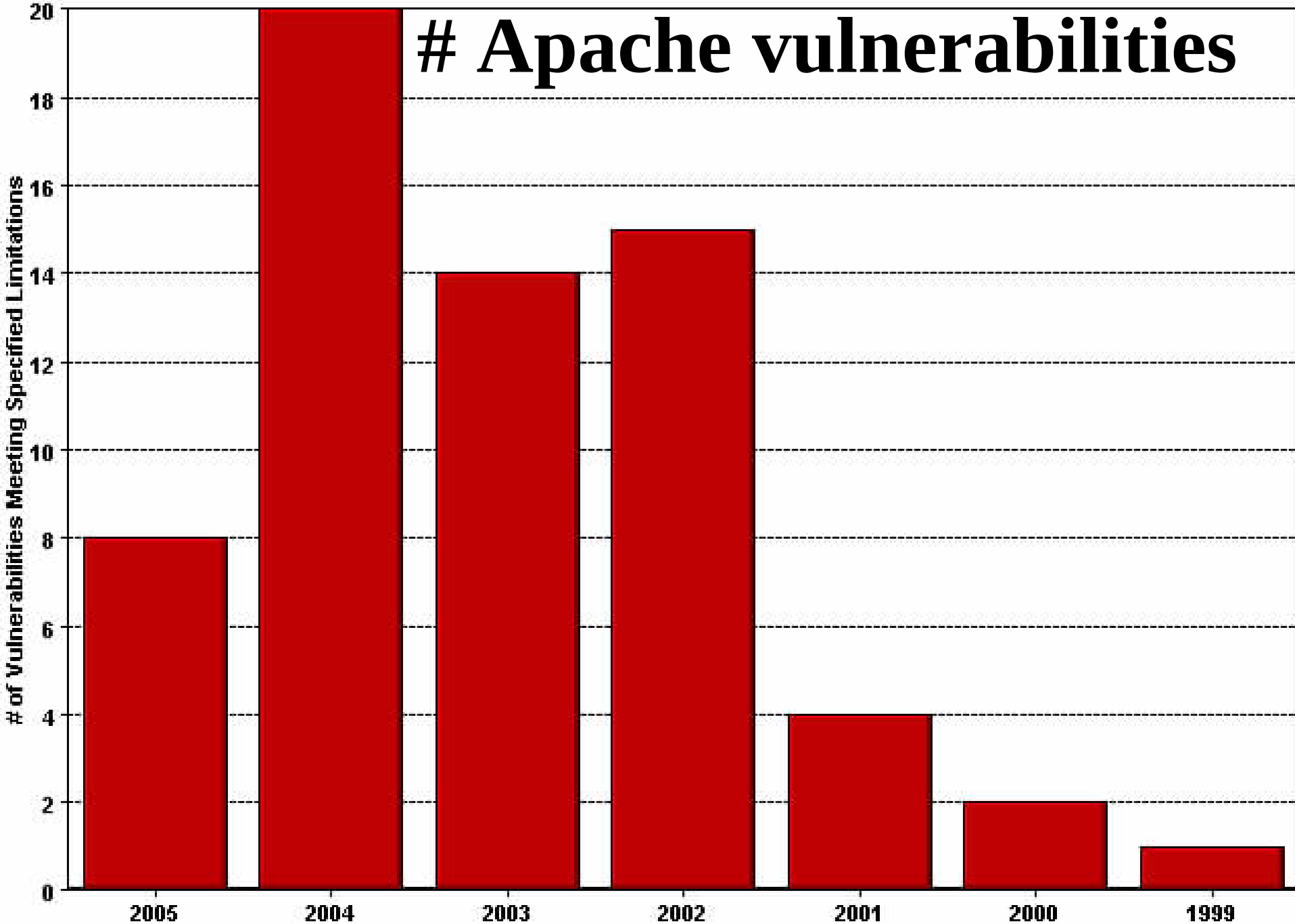
- ○ US-CERT Technical Alerts
- ○ US-CERT Vulnerability Notes
- ○ US-CERT Technical Alerts or Vulnerability Notes
- ○ OVAL Queries

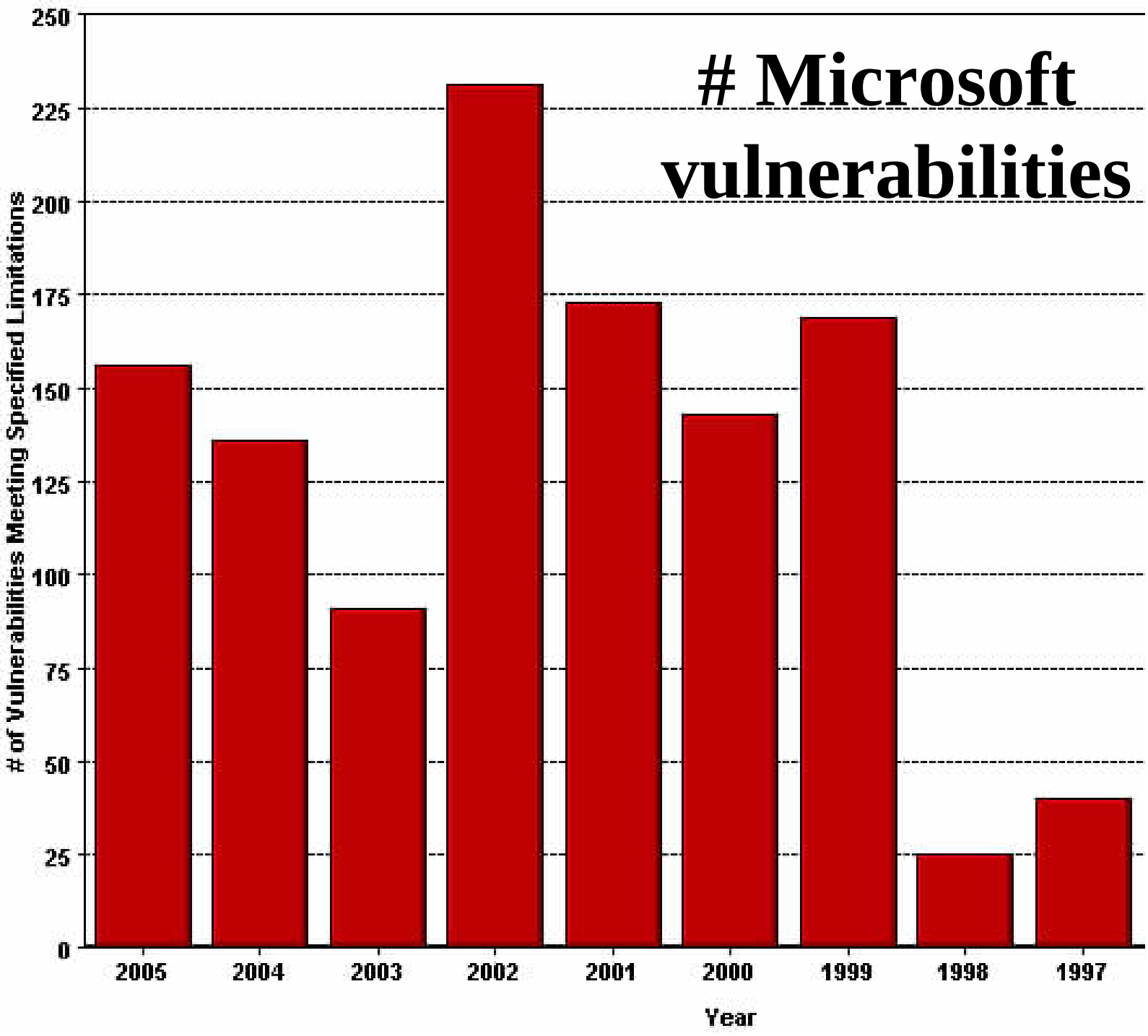
Calculate Statistics

Total # of vulnerabilities

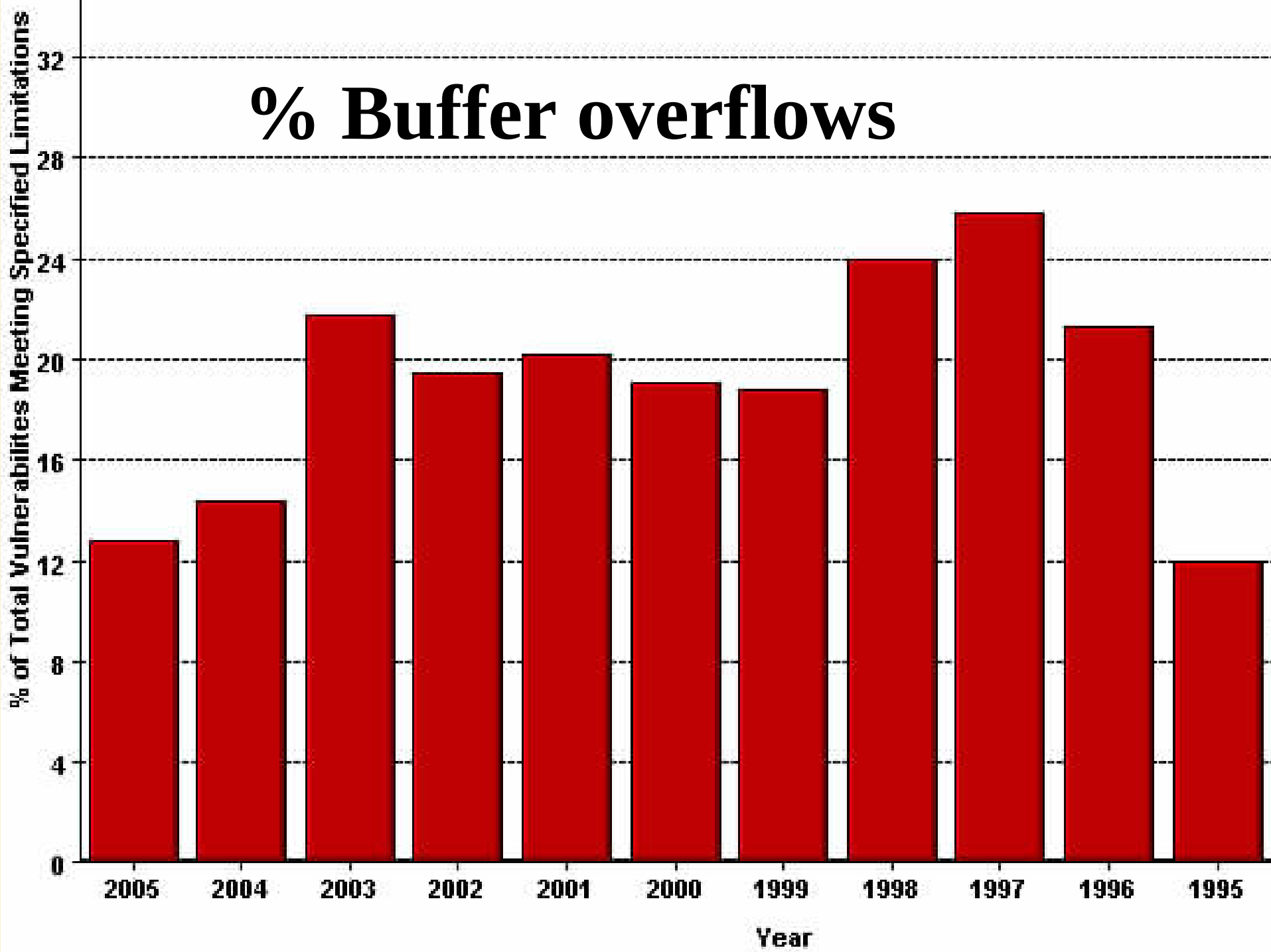



# of IIS vulnerabilities
# of Vulnerabilities Meeting Specified Limitations
40
36
32
28
24
20
16
12
8
4
0
2005
2004
2003
2002
2001
2000
1999
1998
1997
1996
Year


Apache vulnerabilities
of Vulnerabilities Meeting Specified Limitations
0
2
4
6
8
10
12
14
16
18
20
2005
2004
2003
2002
2001
2000
1999


Microsoft vulnerabilities
of Vulnerabilities Meeting Specified Limitations
250
225
200
175
150
125
100
75
50
25
0
2005
2004
2003
2002
2001
2000
1999
1998
1997
Year

% Buffer overflows



CVSS Overview

- Common Vulnerability Scoring System (CVSS)
- A universal language to convey vulnerability severity and help determine urgency and priority of response
- Solves problem of multiple, incompatible scoring systems in use today
- Initially a NIAC project
  - Subgroup of the global Vulnerability Disclosure Framework WG
  - Now under the custodial care of FIRST
- Open
- Usable, understandable, and dissectible by anyone

FIRST CVSS:

http://www.first.org/cvss/

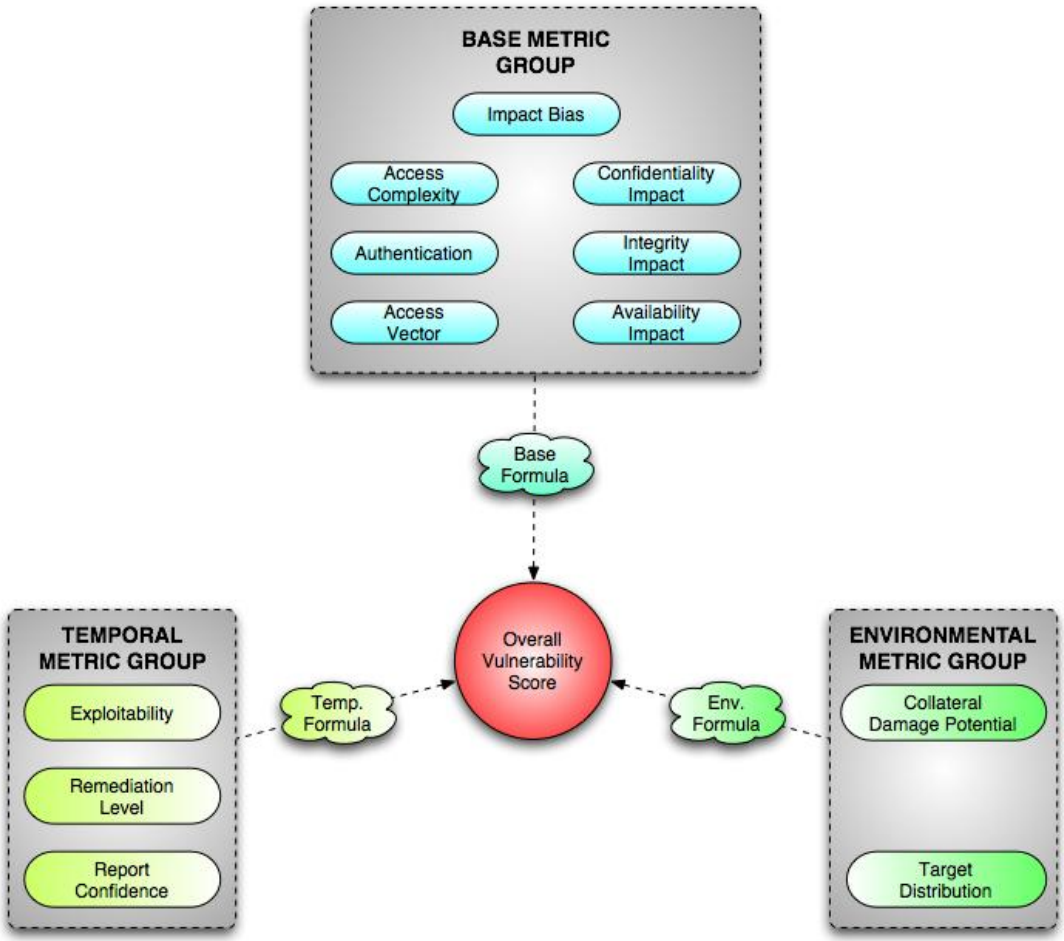
NVD CVSS Portal:

http://nvd.nist.gov/cvss.cfm

Why CVSS?

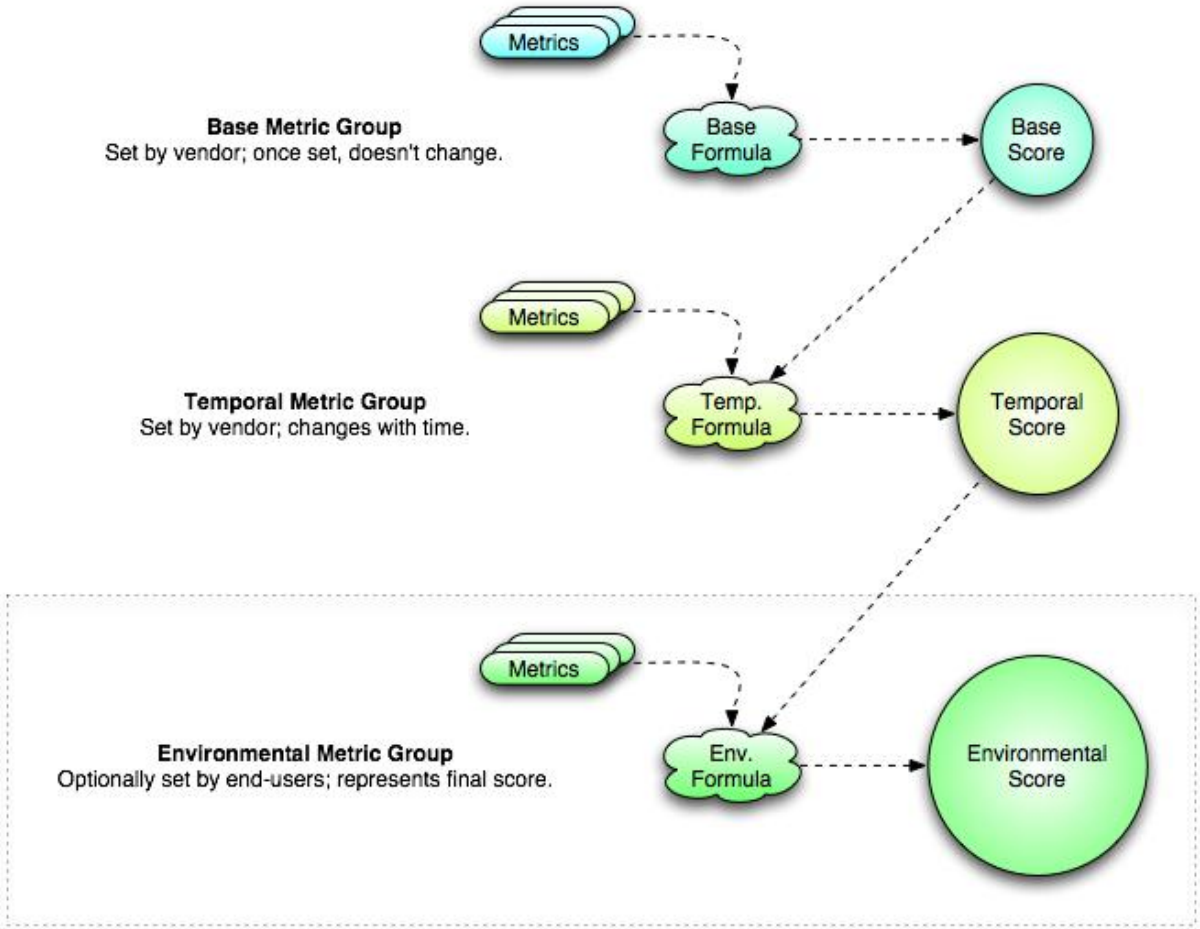
- Different Organizations
  - Vendors (response)
  - Coordinators (notification, coordination)
  - Reporters (research, discovery)
  - Users (mitigation)
- All have different roles, motivations, priorities, resources, etc
- We need a common way to communicate!

CVSS (Metrics View)



FIRST™
Improving Security Together

CVSS (Scoring View)



FIRST™
Improving Security Together

Common Vulnerability Scoring System Sample Vulnerabilities

Vulnerability Common Name	Cisco IOS Interface Blocked DoS	Microsoft LSASS	Microsoft Outlook Express Scripting
CVE reference	CAN-2003-0567 (IOS DOS)	CAN-2003-0533 (Sasser Worm)	CAN-2004-0380
Vulnerability Details	http://www.cisco.com/en/US/products/products_security_advisory09186a00801a34c2.shtml	http://www.securityfocus.com/bid/10108	http://www.securityfocus.com/bid/9105
Access Vector	REMOTE	REMOTE	REMOTE
Access Complexity	LOW	LOW	HIGH
Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED
Confidentiality Impact	NONE	COMPLETE	COMPLETE
Integrity Impact	NONE	COMPLETE	COMPLETE
Availability Impact	COMPLETE	COMPLETE	COMPLETE
Impact Bias	AVAILABILITY	NORMAL	NORMAL
BASE SCORE	**5.0**	**10.0**	**8.0**
Exploitability	HIGH	HIGH	HIGH
Remediation Level	OFFICIAL-FIX	OFFICIAL-FIX	OFFICIAL-FIX
Report Confidence	CONFIRMED	CONFIRMED	CONFIRMED
TEMPORAL SCORE	**4.4**	**8.7**	**7.0**
Collateral Damage Potential	NONE	NONE	LOW
Target Distribution	HIGH	HIGH	HIGH
ENVIRONMENTAL SCORE	**4.4**	**8.7**	**7.3**

Scoring and Formulas

- The process of combining metric values
- Base score is the “foundation”
  - Modified by Temporal and Environmental metrics
- Base and Temporal scores computed by vendors and coordinators with the intent of being published
- Environmental score optionally computed by end-user / organization

Example Vulnerability

NVD
nvd.nist.gov

Vulnerability Summary CVE-2005-3934

Original release date: 12/1/2005
Last revised: 12/1/2005
Source: US-CERT/NIST

Overview

Buffer overflow in Symantec pcAnywhere 11.0.1, 11.5.1, and all other 32-bit versions allows remote attackers to cause a denial of service (application crash) via unknown attack vectors.

Impact

CVSS Severity: 2.5 (Low)
Range: Remotely exploitable
Authentication: Not required to exploit
Impact Type: Allows disruption of service

References to Advisories, Solutions,

External Source: (disclaimer)
Type: Advisory , **Patch Information**
Hyperlink: http://www.symantec.com/avcenter/

External Source: BID (disclaimer)
Name: 15646
Type: Advisory
Hyperlink: http://www.securityfocus.com/bid/15

Vulnerable software and versions

Symantec, pcAnywhere, 11.5.1
Symantec, pcAnywhere, 11.5
Symantec, pcAnywhere, 11.0.1
Symantec, pcAnywhere, 11.0
Symantec, pcAnywhere, 10.5
Symantec, pcAnywhere, 10.0
Symantec, pcAnywhere, 9.2
Symantec, pcAnywhere, 9.0.1
Symantec, pcAnywhere, 9.0
Symantec, pcAnywhere, 8.0.2
Symantec, pcAnywhere, 8.0.1

Technical Details

CVSS Base Score Descriptor: (AV:R/AC:L/Au:NR/C:N/I:N/A:C/B:I)

Vulnerability Type: Buffer Overflow

CVE Standard Vulnerability Entry:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3934

NVD CVSS Calculator – NVD Provided Scoring

NVD
nvd.nist.gov

CVSS Scoring Page (CVE-2005-3934)

This page shows the components of the CVSS score for CVE-2005-3934 and allows you to refine the base CVSS score provided by NVD. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores.

Update Scores | Reset Scores

CVSS Base Score	2.5
CVSS Temporal Score	Undefined
CVSS Environmental Score	Undefined
Overall CVSS Score	**2.5**

Base Score Metrics

AccessVector	Remote
AccessComplexity	Low
Authentication	Not Required
ConfImpact	None
IntegImpact	None
AvailImpact	Complete
ImpactBias	Weight integrity

Environmental Score Metrics

CollateralDamagePotential	Undefined
TargetDistribution	Undefined

Temporal Score Metrics

Exploitability	Undefined
RemediationLevel	Undefined
ReportConfidence	Undefined

CVSS Vector

This vector displays in a concise format the base and temporal inputs to the CVSS score.

(AV:R/AC:L/Au:NR/C:N/I:N/A:C/B:I/E:?/RL:?/RC:?)

NVD CVSS Calculator – Temporal and Environmental Scoring

NVD
nvd.nist.gov

CVSS Scoring Page (CVE-2005-3934)

This page shows the components of the CVSS score for CVE-2005-3934 and allows you to refine the base CVSS score provided by NVD. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores.

Update Scores | Reset Scores

CVSS Base Score	2.5
CVSS Temporal Score	1.8
CVSS Environmental Score	1.1
Overall CVSS Score	**1.1**

Base Score Metrics

AccessVector	Remote
AccessComplexity	Low
Authentication	Not Required
ConfImpact	None
IntegImpact	None
AvailImpact	Complete
ImpactBias	Weight integrity

Environmental Score Metrics

CollateralDamagePotential	Medium (significant loss)
TargetDistribution	Low (0-25%)

Temporal Score Metrics

Exploitability	Unproven that exploit exists
RemediationLevel	Official fix
ReportConfidence	Confirmed

CVSS Vector

This vector displays in a concise format the base and temporal inputs to the CVSS score.

(AV:R/AC:L/Au:NR/C:N/I:N/A:C/B:I/E:U/RL:O/RC:C)

Industry Adoption

Organization	Status	Organization	Status
Akamai	Adopted	npower	Evaluating
Amazon	Evaluating	RWE	Evaluating
American Water	Adopted	Symantec	Rolling out
ArcSight	Evaluating	Qualys	Rolling out
Cisco	Adopted	Tenable	Rolling out
eBay	Evaluating	Thames Water	Adopted
IBM	Evaluating	Union Pacific	Adopted
McAfee	Evaluating	webMethods	Rolling out
netForensics	Evaluating	CSC	Evaluating

Questions?

- Peter Mell
- 301-975-5572
- mell@nist.gov

NVD
nvd.nist.gov

http://nvd.nist.gov