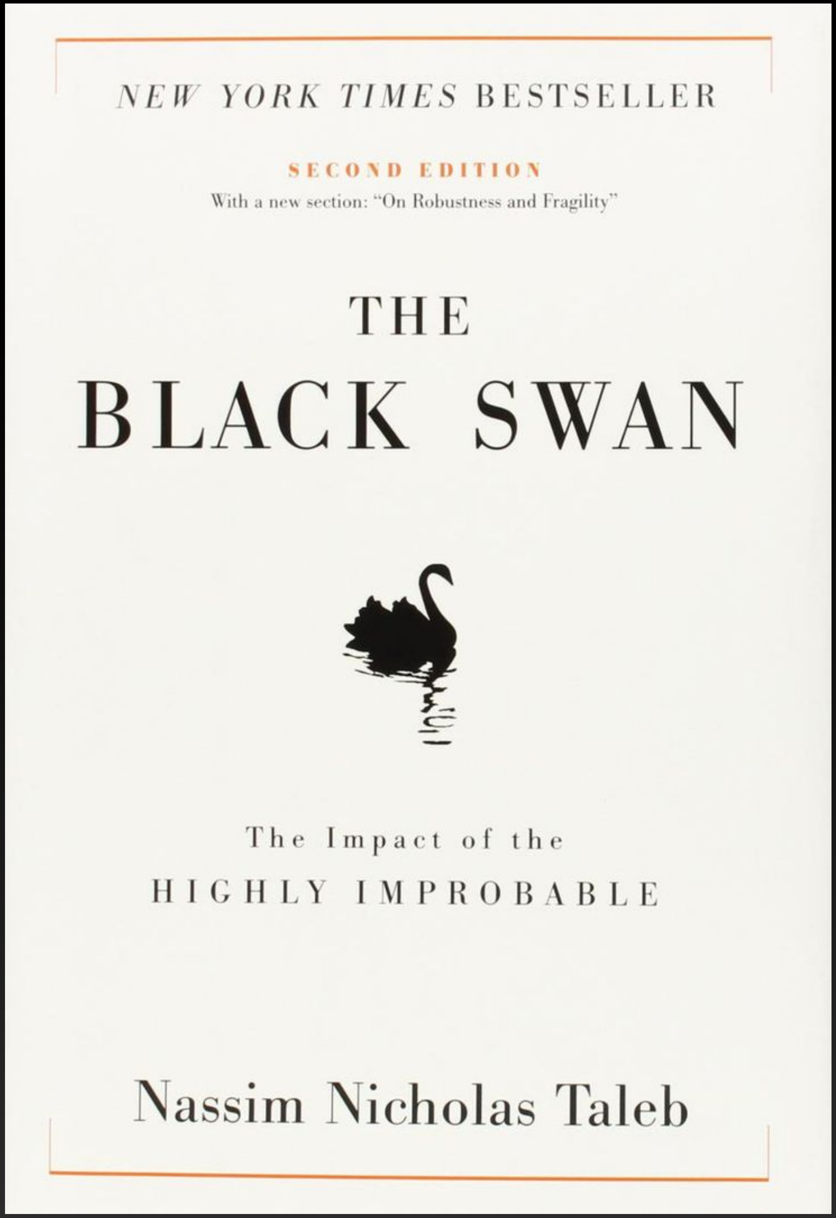
Monsters under the Bitcoin Bed

Jacob Welsh (WoT: jfw)

0CBC 0594 1D03 FD95 C3A4
7654 AE0D F306 0255 94B3

http://fixpoint.welshcomputing.com/



NEW YORK TIMES BESTSELLER

SECOND EDITION

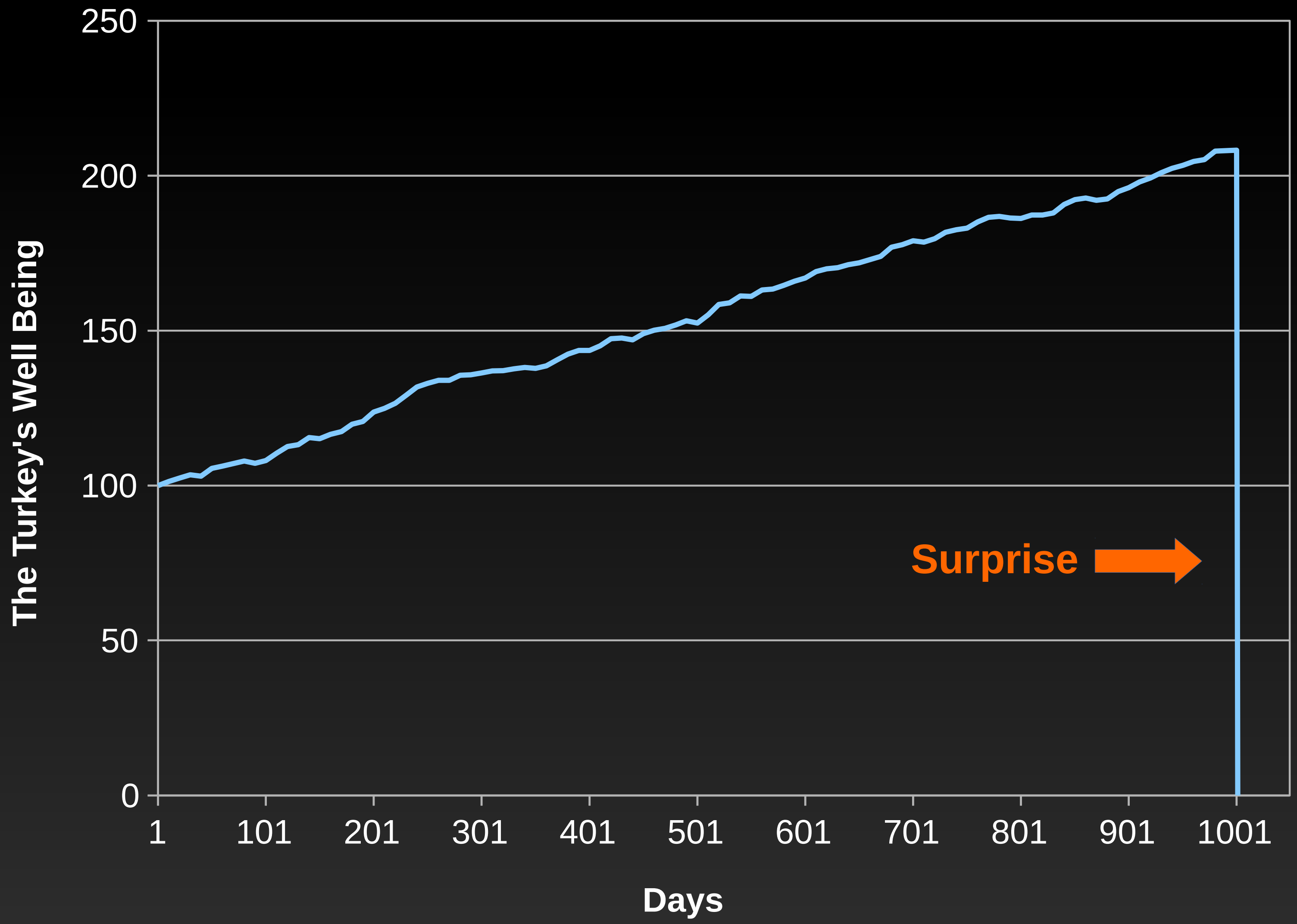
With a new section: "On Robustness and Fragility"

THE BLACK SWAN

The Impact of the HIGHLY IMPROBABLE

Nassim Nicholas Taleb

1000 and 1 days in the life of a Thanksgiving turkey



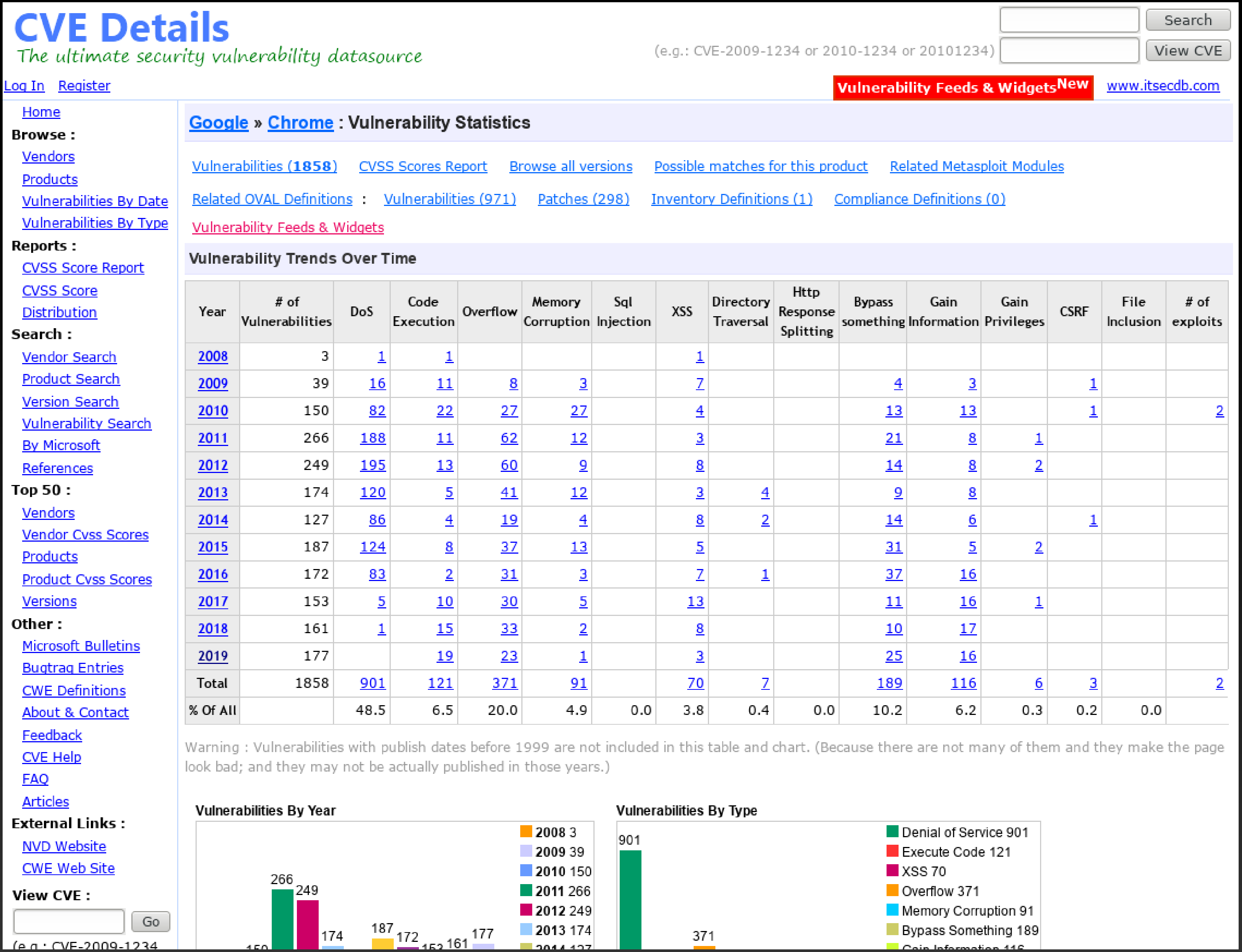
Well-known risks in bitcoin

- Counter-party risk (shady exchanges)
- “Hacking”
  - Buggy, insecure software
  - Weak passwords
  - Social engineering
- Data loss
- Physical theft
- Disinformation
- More?

“Minimize funds held on exchanges”

- But who are your *implicit* counter-parties?
- Are Apple, Microsoft, Google and Intel products fit to secure the world’s digital cash?
- In what power structure do these firms operate?
- How many people you don’t know can touch the code?
- How many people you *do* know are vetting the code?
- How much code *is* there?

Can you trust your software today?



CVE Details

The ultimate security vulnerability datasource

Search | (e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register Vulnerability Feeds & Widgets New www.itsecdb.com

- Home
- **Browse :**
  - Vendors
  - Products
  - Vulnerabilities By Date
  - Vulnerabilities By Type
- **Reports :**
  - CVSS Score Report
  - CVSS Score Distribution
- **Search :**
  - Vendor Search
  - Product Search
  - Version Search
  - Vulnerability Search
  - By Microsoft References
- **Top 50 :**
  - Vendors
  - Vendor Cvss Scores
  - Products
  - Product Cvss Scores
  - Versions
- **Other :**
  - Microsoft Bulletins
  - Bugtraq Entries
  - CWE Definitions
  - About & Contact
  - Feedback
  - CVE Help
  - FAQ
  - Articles
- **External Links :**
  - NVD Website
  - CWE Web Site
- **View CVE :**
  - Go
  - (e.g.: CVE-2009-1234

Google » Chrome : Vulnerability Statistics

Vulnerabilities (1858) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (971) Patches (298) Inventory Definitions (1) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

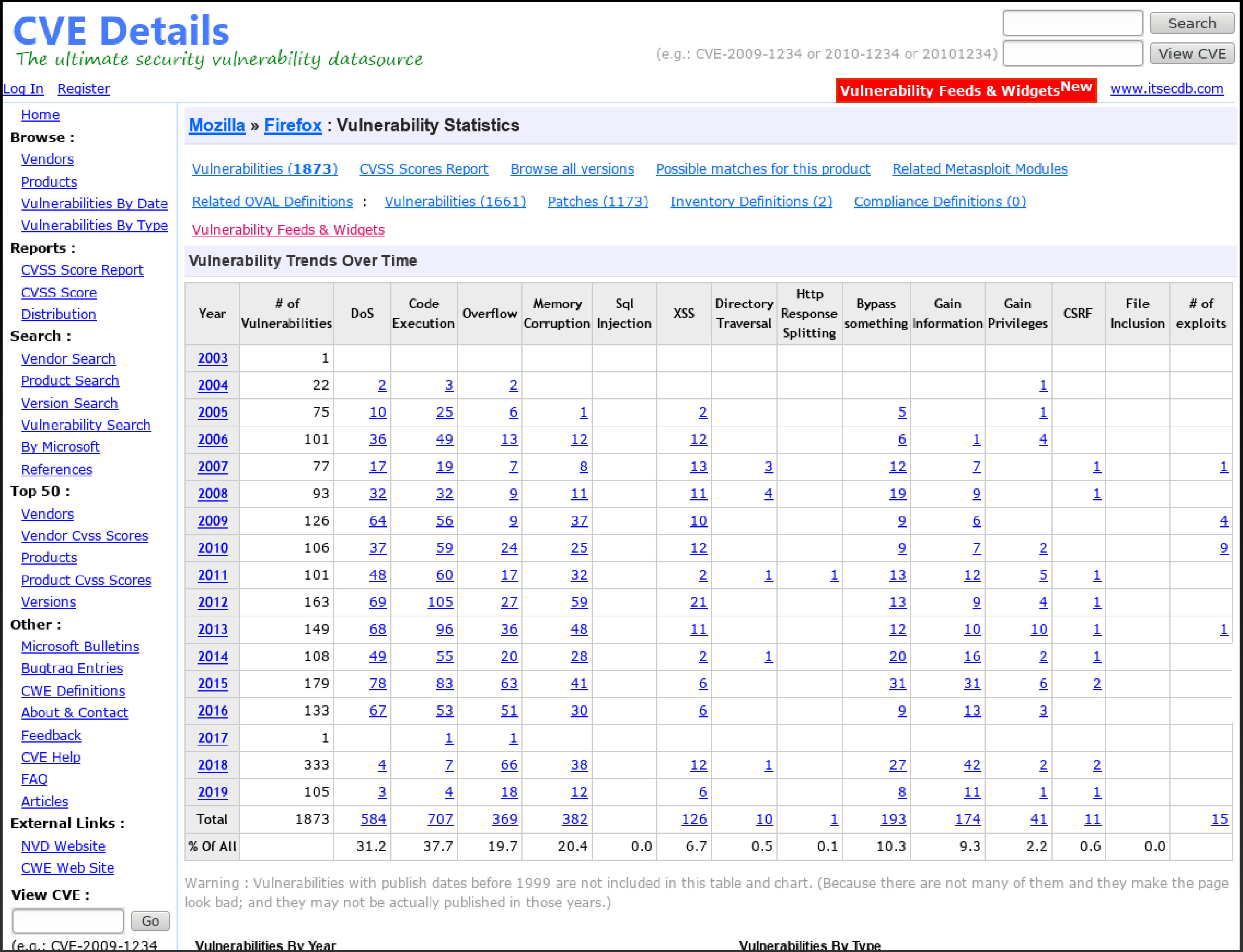
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2008	3	1	1				1								
2009	39	16	11	8	3		7			4	3		1		
2010	150	82	22	27	27		4			13	13		1		2
2011	266	188	11	62	12		3			21	8	1			
2012	249	195	13	60	9		8			14	8	2			
2013	174	120	5	41	12		3	4		9	8				
2014	127	86	4	19	4		8	2		14	6		1		
2015	187	124	8	37	13		5			31	5	2			
2016	172	83	2	31	3		7	1		37	16				
2017	153	5	10	30	5		13			11	16	1			
2018	161	1	15	33	2		8			10	17				
2019	177		19	23	1		3			25	16				
Total	1858	901	121	371	91		70	7		189	116	6	3		2
% Of All		48.5	6.5	20.0	4.9	0.0	3.8	0.4	0.0	10.2	6.2	0.3	0.2	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year

Vulnerabilities By Type

Can you trust your software today?



CVE Details

The ultimate security vulnerability datasource

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

NVD Website

CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234

Mozilla » Firefox : Vulnerability Statistics

Vulnerabilities (**1873**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (1661) Patches (1173) Inventory Definitions (2) Compliance Definitions (0)

Vulnerability Feeds & Widgets

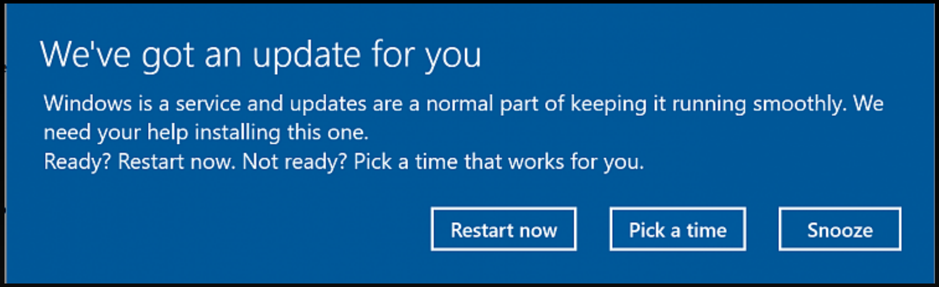
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2003	1														
2004	22	2	3	2								1			
2005	75	10	25	6	1		2			5		1			
2006	101	36	49	13	12		12			6	1	4			
2007	77	17	19	7	8		13	3		12	7		1		1
2008	93	32	32	9	11		11	4		19	9		1		
2009	126	64	56	9	37		10			9	6				4
2010	106	37	59	24	25		12			9	7	2			9
2011	101	48	60	17	32		2	1	1	13	12	5	1		
2012	163	69	105	27	59		21			13	9	4	1		
2013	149	68	96	36	48		11			12	10	10	1		1
2014	108	49	55	20	28		2	1		20	16	2	1		
2015	179	78	83	63	41		6			31	31	6	2		
2016	133	67	53	51	30		6			9	13	3			
2017	1		1	1											
2018	333	4	7	66	38		12	1		27	42	2	2		
2019	105	3	4	18	12		6			8	11	1	1		
Total	1873	584	707	369	382		126	10	1	193	174	41	11		15
% Of All		31.2	37.7	19.7	20.4	0.0	6.7	0.5	0.1	10.3	9.3	2.2	0.6	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

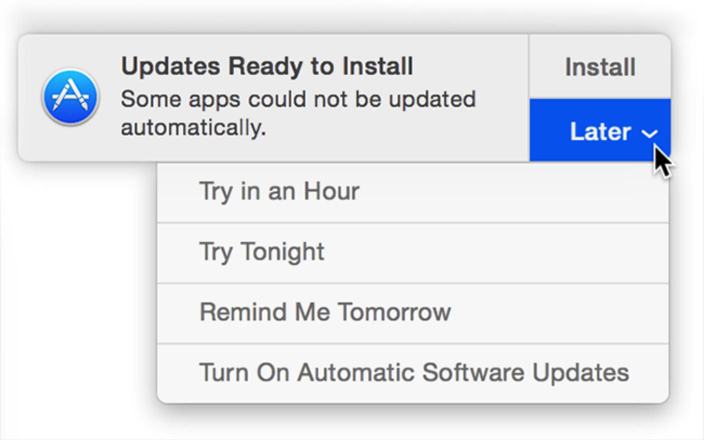
Vulnerabilities By Year **Vulnerabilities By Type**

Can you trust your software tomorrow?

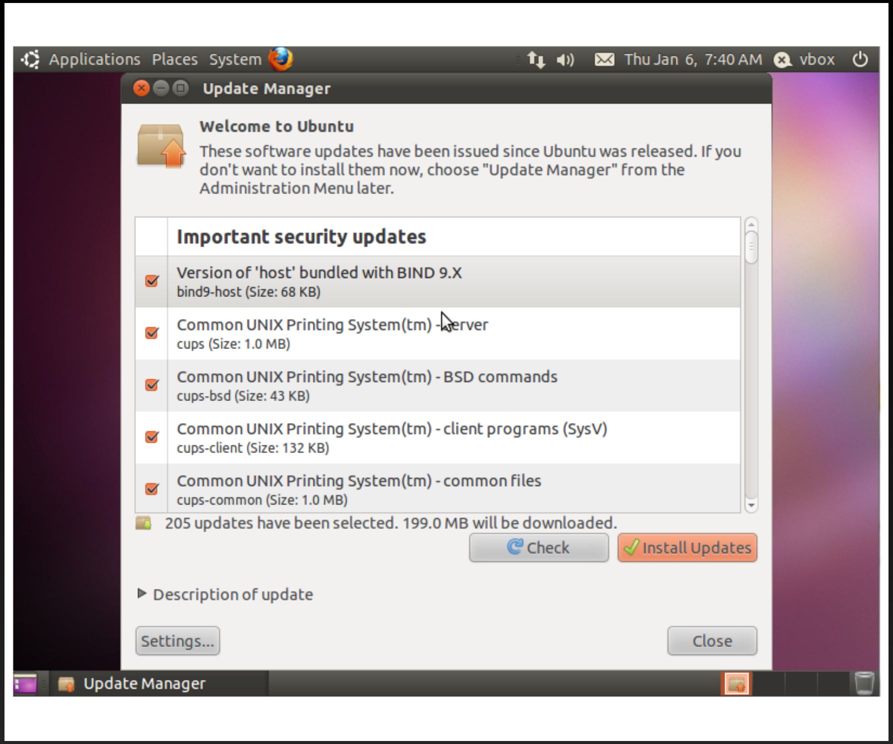


We've got an update for you

Windows is a service and updates are a normal part of keeping it running smoothly. We need your help installing this one.
Ready? Restart now. Not ready? Pick a time that works for you.



Updates Ready to Install
Some apps could not be updated automatically.



Welcome to Ubuntu
These software updates have been issued since Ubuntu was released. If you don't want to install them now, choose "Update Manager" from the Administration Menu later.

Important security updates

- ☑ Version of 'host' bundled with BIND 9.X
  bind9-host (Size: 68 KB)
- ☑ Common UNIX Printing System(tm) - server
  cups (Size: 1.0 MB)
- ☑ Common UNIX Printing System(tm) - BSD commands
  cups-bsd (Size: 43 KB)
- ☑ Common UNIX Printing System(tm) - client programs (SysV)
  cups-client (Size: 132 KB)
- ☑ Common UNIX Printing System(tm) - common files
  cups-common (Size: 1.0 MB)

205 updates have been selected. 199.0 MB will be downloaded.

Cold storage and hardware wallets

- How good are typical “paper” wallets?
  - Still need PC to generate keys
  - Still need online PC to spend the funds
- How good are typical “hardware” wallets?
  - Still need online PC to operate, exposing to bad **input** and **side-channel attacks** (power, timing)
  - Mass-market products with complex software stacks, security flaws and blind-trust **firmware updates**
  - Unverifiable **entropy sources**

Cryptographic entropy

- Numbers that can’t be predicted with any better odds than random guessing
- Required for cryptographic keys and strong passwords
- Cannot be obtained by algorithmic means; must come from **nature**
- **Statistical** randomness is implied but it alone is not sufficient
  - I.e., not enough to **look** random
  - Folly of RNG “whitening”
  - Rolling dice is likely better than whatever you’re doing now

Deliberately compromised hardware

- Intel Management Engine (2009)
- AMD Platform Security Processor (2013)
- UEFI firmware and “Secure Boot”
- ARM TrustZone, often opaque boot firmware
- Alternative architectures mostly confined to large-scale or low-power markets

Fast food computing

- For decades, the industry has increasingly served the *fast food computing* paradigm, catering to a mass market that values:
  - Superficially pleasing, **black box** products that work **most** of the time
  - Usability without having to **think**
  - Latest & greatest bells & whistles
  - Cheapness of products and labor
- The *home-cooked computing* paradigm instead favors:
  - Open and **comprehensible** source code
  - **Small-scale** production
  - Eliminating excess **complexity**
  - Attention to **detail**
  - Doing things **yourself**
  - Building **relationships** with experts

JWRD Computing

- Founded 2016 on a mission to assist clients in realizing personal sovereignty through strengthening digital security.
- We provide qualified individuals a relatively sane, customizable computing environment, set of key management tools, and an in-depth, one-on-one training program to use them effectively.
- We began publishing about our work in late 2019 and have since gained favorable recognition and support from the Bitcoin elite as witnessed by the Web of Trust.

Practical solutions at every layer

- Hardware
  - Fully refurbished, field-serviceable, unlocked **ThinkPads**
  - 3-port gigabit firewall **router**
  - Verifiable **random number generator**
  - Fiber-optic **data diode** for airgapping
- Operating system
  - Custom built, blob-free **Coreboot** firmware on ThinkPads
  - **Gales Linux**, a no-nonsense distribution built fully from source code
  - **Kernel configuration** tailored to the hardware
  - Custom **OpenBSD** install on routers
- Software development
  - **V**, a cryptographic source code manager making trust decisions explicit
  - **Gales Scheme**, a small yet powerful interpreter
- Application
  - **GPG** true end-to-end communications security
  - **yrc** no-nonsense real-time chat
  - **The Real Bitcoin** (TRB) fully verifying node
  - Innovative TRB- and airgap-friendly **Gales Bitcoin Wallet**

Active Learning methodology

- The typical lesson features:
  - Warm-up activity
  - Presentation of new concepts
  - Cueing to stimulate recall
  - Guided practice to integrate the new information
- Homework includes:
  - Background readings
  - Independent practice exercises
- Complex abstractions are broken down into simple parts aided by whiteboard, pen and paper, and demonstrations
- Knowledge is converted into action

We come to you

- Training sessions held in the client's home or office, one-on-one or in small groups
  - Virtual classroom can be considered where this is not possible.
- No advance computing knowledge required
  - We start where you're at and move at the pace that's right for you.
  - Instruction and supporting materials are in English.
- The successful client is a lifelong learner with the patience, humility and commitment to learn.

Side benefits

- Build relationships in a network of elite and active individuals
- Expert tools and clear thinking open a new world of business solutions
  - **mircea_popescu:** the fundamental problems are that cli-iliteracy is a serious, life-changing disability. in terms of severity, blindness compares, deafness does not. obviously the afflicted are scarcely aware, but this doesn't mean they're not afflicted.
  - **mircea_popescu:** whole "work-years", entire "departments" could readily be replaced by you know, half hour's worth of sed ; they aren't because us corporatelandia mostly exists as makework, to create the illusion for millions of ambitious derps that they're "doing something" lest they take to the streets and start throwing rocks. nevertheless, even if the cutting legs is systematically needed in socialism, to crate the sort of helpless vat-people it can thrive amongst, it's still personally disabling.
  - **mircea_popescu:** so you know, as far as the life prospects, the future evolution, however you will name the sum-total potential of a person's existence, understanding how to command line is more important than meeting their father. it'll certainly do a lot for them, and it certainly CAN do way the fuck more for them.

“So my friends : do not be afraid of all the things that are scary. The most they can do while under your gaze is make you stronger. Be instead afraid of the things you make no effort to understand, because from behind they can give you quite the sound trashing. And the worst part of it is... you'll likely never know.”

- Mircea Popescu

http://trilema.com/a-conceit-or-the-importance-of-blogging

The time to act is now.

- The next 10x devaluation of fiat against Bitcoin may be around the corner. Are you ready for what that might mean?
- Learning better tools and habits takes time, effort, and competent guidance.
- Shine your light and let the monsters scurry.
- Don’t be the turkey.