Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS559
Vulnerabilities



CSU Cybersecurity Center
Computer Science Dept

Probability

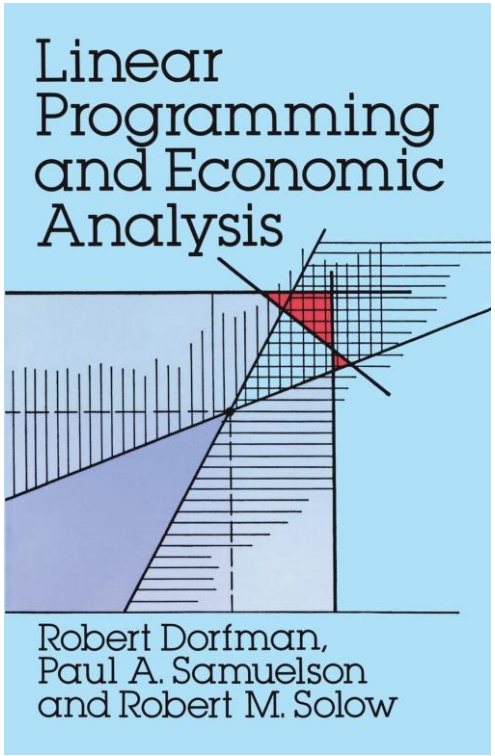
- Disjoint, Independence, Bayes' rule
- Confusion Matrix, various measures
- Common distributions: continuous, discrete
- Stochastic processes: Markov, Poisson

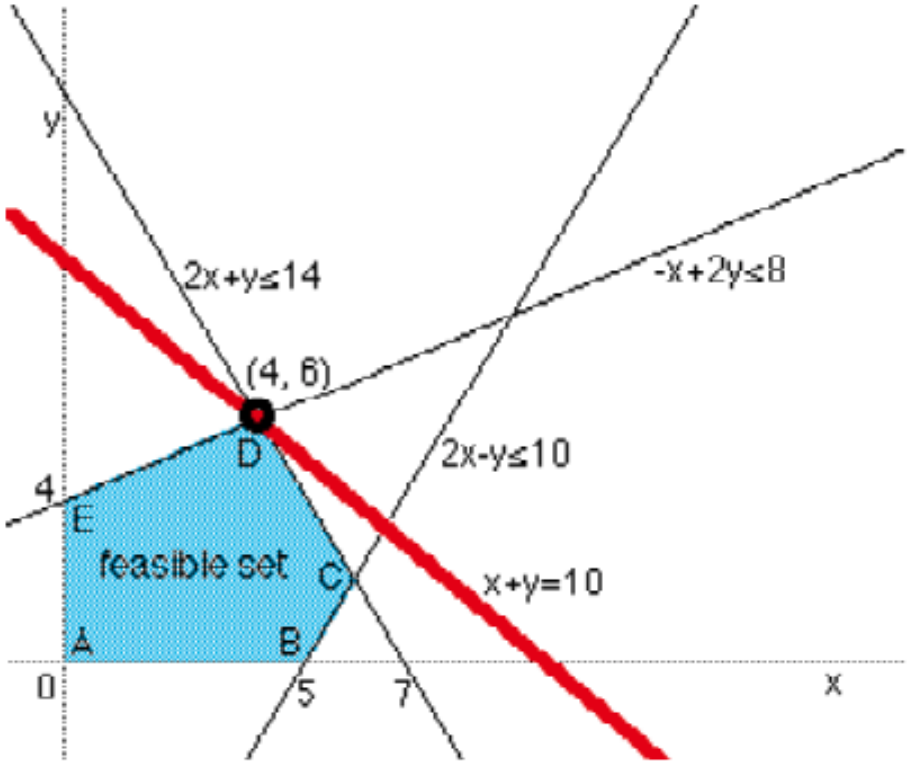
Modeling and regeression

- Curve fitting: linear, polynomial, logarithmic, exponential etc.
  - Goodness of fit vs predictive capability
- Using mathematical formulas
- Using excel
  - functions linest( ), logest( )
  - Trendline

Linear, Nonlinear Programming

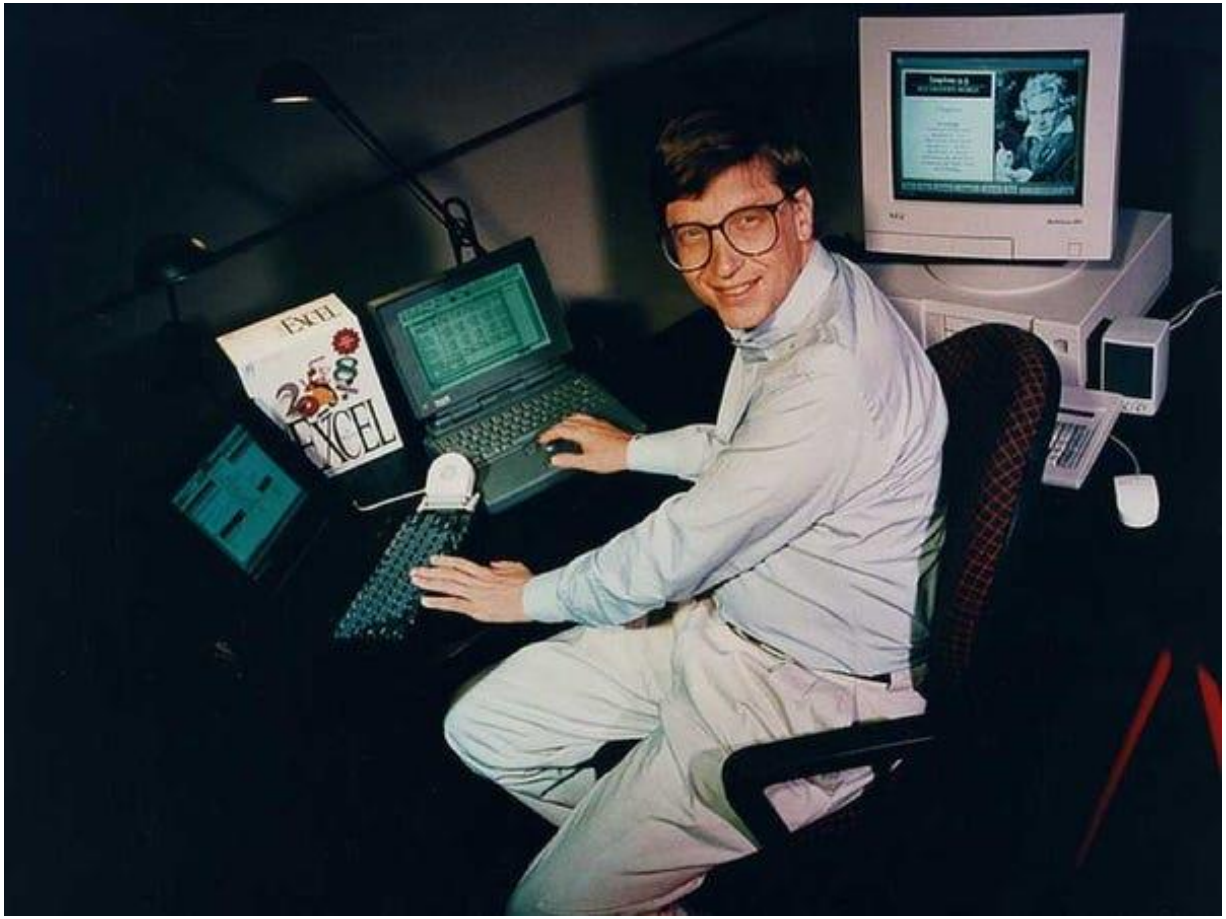
Maximize x+y with the given constraints.





Colorado State University

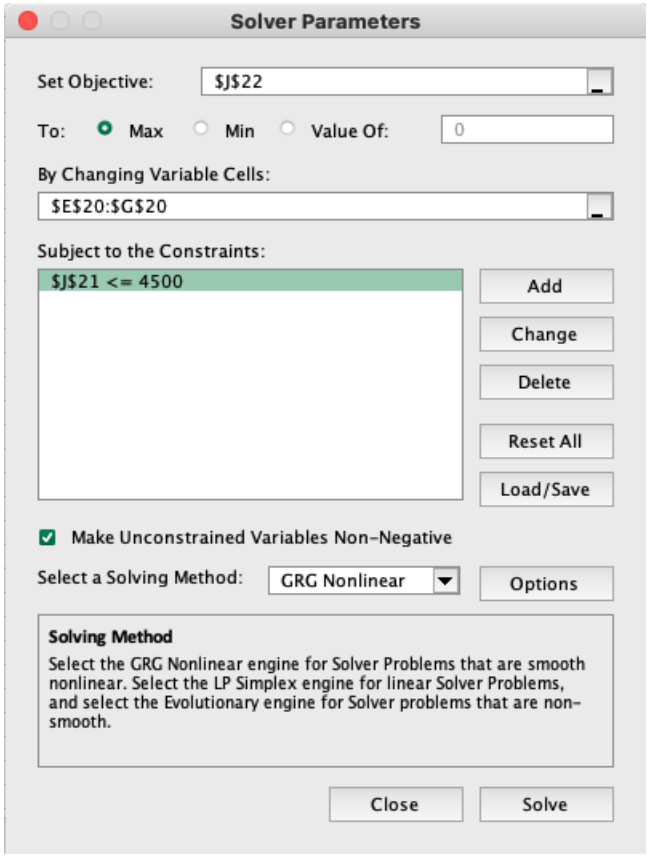
Excel Magic



Colorado State University

Excel Solver

- You need to install add-in in your excel so that it shows up in the Data menu.
- Set up an optimization problem
  - What to optimize (e.g. minimize least square error)
  - Constraints to satisfy
  - Specify initial estimates of parameters
- Iterative solution (choice of algorithms)
- Result may depend on initial values for non-linear fitting.



Colorado State University

Classic Optimization Problem

- Linear Programming, Non-Linear Programming etc.
- Specified
  - Objective function: minimize or maximize
  - Constraints: equalities, inequalities
- Generally solution is iterative
- Excel Solver algorithms
    - Simplex method is used for solving linear problems
    - GRG solver for solving smooth nonlinear problems
    - Evolution solver uses genetic algorithms
- Excel solver for curve fitting
  - Minimize error (square of differences between model and actual data points)
  - Some constraints(e.g. parameters may be required to be positive0

Initial Values

- Start with some initial values and the gradually iterate towards optimal.
- When 3 or more parameters are used, it is best to start with some good initial guesses.
- Algorithm may get stuck at a local minimum/maximum
- Repeat with diverse initial guesses.

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS559
Vulnerabilities



CSU Cybersecurity Center
Computer Science Dept

Security Holes: Types

- Software holes: Vulnerabilities
  - CVSS scores involving *exploitability* and *impact* is a type of risk measure.
- System/physical holes
- Personnel/Procedural holes:
  - e.g. Phishing
- Exploitation may involve multiple holes, perhaps of different types
  - Understanding and classify them:
    - Target 2013 breach: credentials stolen from a HVAC contractor
    - Equifax 2017 breach: vulnerability patch not applied

Defects vs vulnerabilities

- Software defects vs Vulnerabilities
  - Defect: any defect
  - Vulnerability: security related defect, perhaps 1-5% of defects
- Testing for defects or vulnerabilities:
  - Defects: Apply inputs to ensure the output is as expected
    - Or examine code to look for flaws
  - Vulnerabilities: Apply inputs to see if they cause unexpected behavior
    - Or examine code to look for flaws
- When are the discovered
  - prior to release by developer
  - Field testing: developers, users, bug-hunters

Risks due to vulnerabilities

- **Risk** due to an adverse event e_i

  $Risk_i = Likelihood_i \times Impact_i$

- $Likelihood_i$ = P{A security $hole_i$ is exploited}.

  = P{$hole_i$ present}.

  P{exploitation | $hole_i$ present}

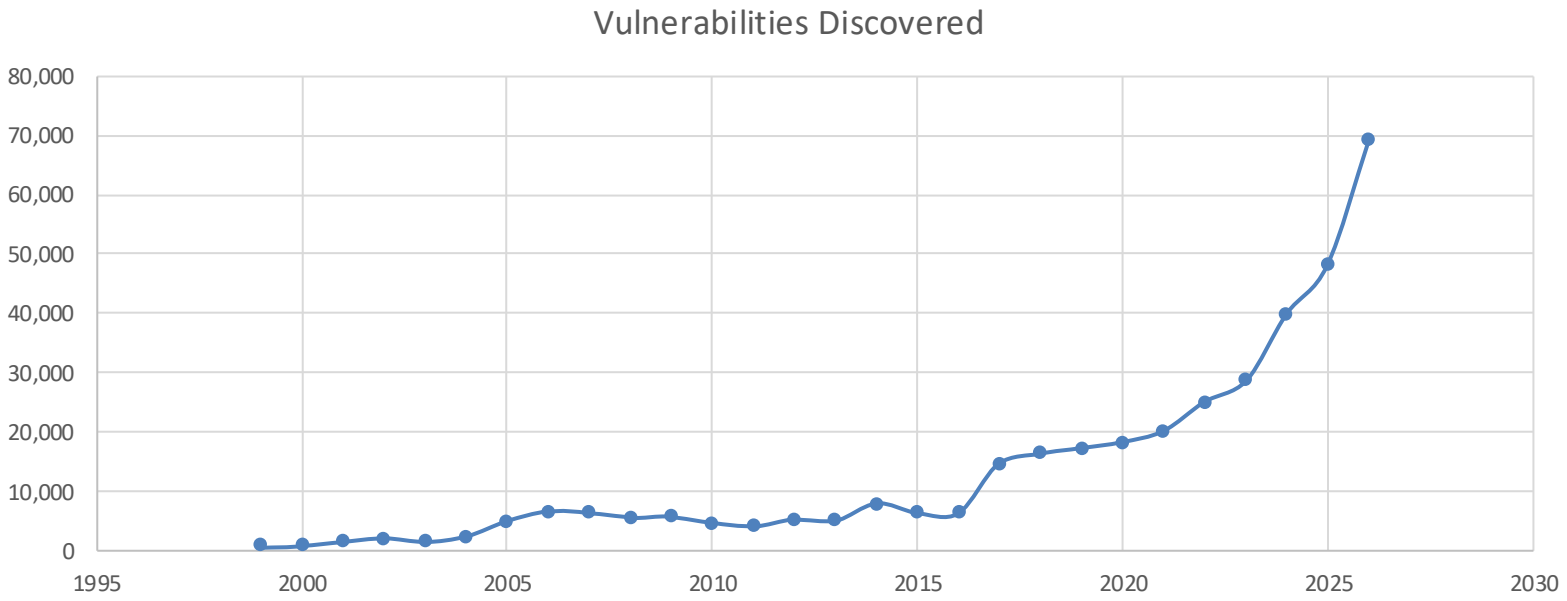
  - P{$hole_i$ present}: an internal attribute of the system.
  - P{exploitation | $hole_i$ present}: depends on circumstances outside the system.

Components of Likelihood of Exploitation

- Internal
  - Presence of a vulnerability (Vulnerability Discovery*)
  - Vulnerability not patched
- External
  - Attacker's motivation level
  - Technical capabilities, exploit availability*
  - Network access to vulnerable system
- Interface
  - Attack surface* of vulnerable system
  - Reachability* of vulnerability

We have published research related to these. See publications from 2005

Vulnerability Discovery Trend



Vulnerability Data-bases

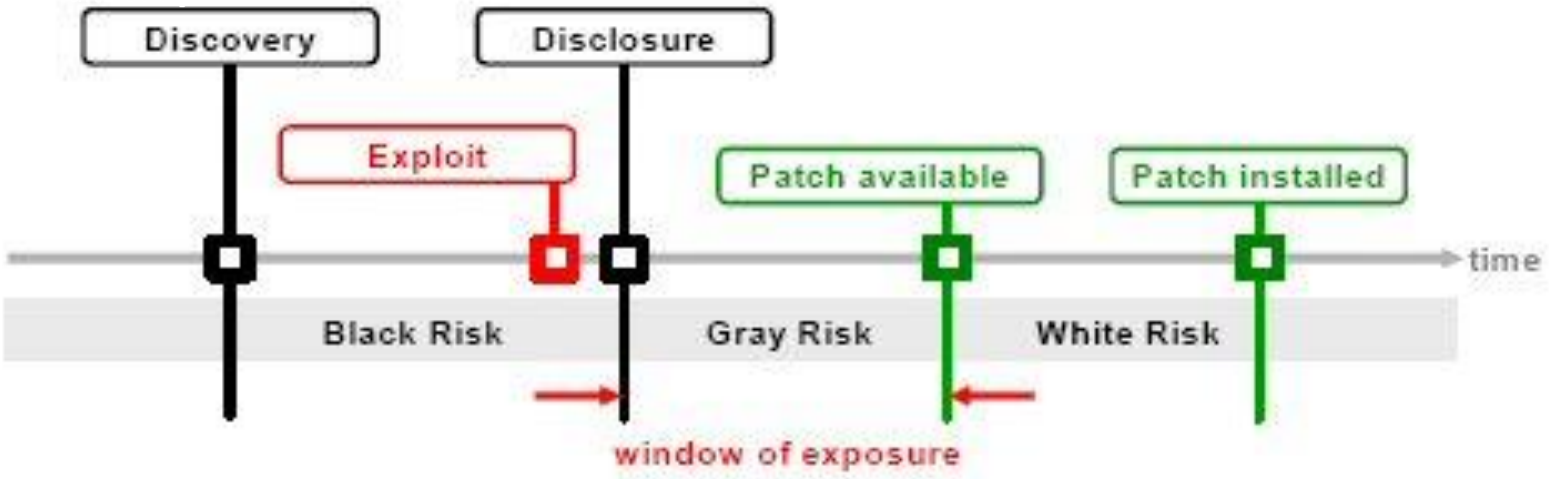
NVD database
CVEDetails
VulnDB
ExploitDB

2026: only partial data. Note the **jump in 2026**.
My theory: AI has made finding vulnerabilities easier

Why the jump in 2017?
More extensive collection by NVD?

Colorado State University

Vulnerability Lifecycle



- Add: creation of a vulnerability
- Exploit can be created before or after disclosure
- Many vulnerabilities are often inherited from a previous version.

15

Vulnerability density and defect density

- **Vulnerability densities**: 95/98: 0.003-0.004 NT/2000/XP: 0.01-0.02
- V_{KD}/D_{KD}: 0.75-2.31% about 1-5%

System	MSLOC	Known Defects (1000s)	D_{KD} (/Kloc)	Known Vulner - abilies	V_{KD} (/Kloc)	Ratio V_{KD} /D_{KD}
Win 95	15	5	0.33	45	0.0031	0.90%
NT 4.0	16	10	0.625	231	0.0144	2.31%
Win 98	18	10	0.556	109	0.0060	1.09%
Win2000	35	63	1.8	637	0.0182	1.01%
Win XP	40	600	15	1352	0.0338	0.23%*
Win 10	65	1000	15.38	7458	0.1147	0.75%

Updated in 2026 from Alhazmi, Malaiya, Ray, " Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems," Computers and Security, May 2007, P 219-228. Note many vulnerabilities are inherited from a previous version, and are discovered much later.

Colorado State University

Who discovers vulnerabilities?

Discoverers	Safari's Vulnerabilities	Percentage	Chromium's Vulnerabilities	Percentage
Product's company discoverers	17	20%	0	0%
Product's company discoverers and others	0	0%	35	35%
Outside discoverers	66	80%	63	64%
Unknown Discoverers	0	0%	1	1%

Vulnerability discoverers from July. 1, 2012 to December 31, 2012: insiders or outsiders

Q: What do outside discoverers do after they have discovered a vulnerability?

A. M. Algarni, and Y. K. Malaiya, "Most Successful Vulnerability Discoverers: Motivation and Methods", Int. Conference on Security and Management (SAM 2013), Las Vegas, July 2013, pp. 3-9.

THE TOP VULNERABILITIES DISCOVERERS ON OSVDB

THE TOP VULNERABILITIES DISCOVERERS ON OSVDB

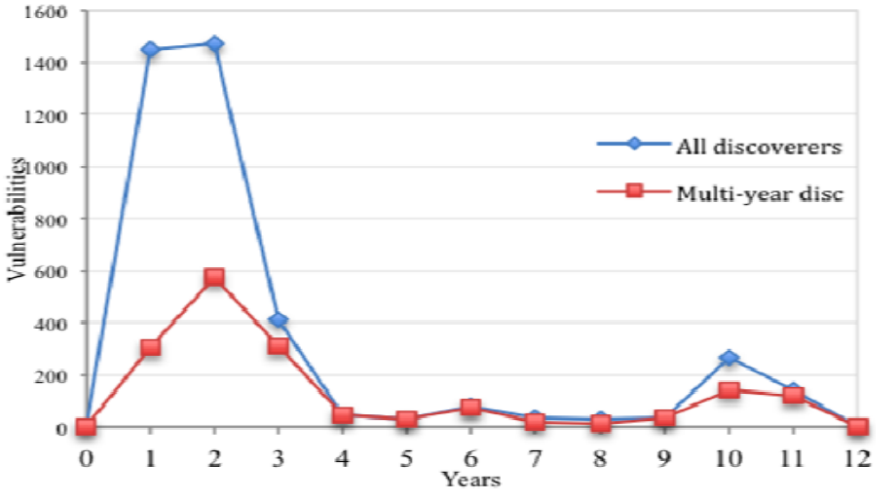
Discoverer	Country	Period	# Vuln	# Vuln types	Why they're interested	Stopped/Continued
r0t	Latvia	2005-08-09 to2010-09-16	810	10	N/A	N/A
Janek Vind "waraxe"	Estonia	2003-08-08 to2013-03-21	319	8	Vulnerability website	N/A
Lostmon Lords	Spain	2004-06-20 to2009-08-15	279	8	Security Researcher	Worked until July 2012
rgod	Italy	2005-06-06 to2012-08-29	277	12	Hacker	Worked until Aug. 2012
Luigi Auriemma	Italy	2000-07-08 to2013-03-16	267	9	Hobby	N/A
Russ McRee	USA	2008-01-14 to 2012-03-02	237	4	Specialist in security	N/A
Aliaksandr Hartsuyeu	Lithuania	2005-12-28 to2011-02-03	229	6	Security Company	Still working 2012
James Bercegay	USA	2003-06-03 to2008-09-04	200	12	Web developer	Worked until 2011
Kacper	Poland	2006-05-12 to2007-08-10	199	3	N/A	N/A
luny	N/A	2006-05-18 to 2006-07-13	142	6	N/A	N/A
Diabolic Crab	N/A	2004-09-25 to 2005-07-12	140	6	N/A	N/A
JeiAr	USA	2003-05-29to 2004-05-04	120	7	Web developer	Worked until 2011
Tan Chew Keong	Singapore	2004-07-29 to 2009-09-28	102	9	Information Security Specialist	N/A
Stefan Esser	Germany	2000-11-09 to 2012-06-03	86	10	Security Consultant	Still do jailbreak until 2012
M.Hasran Addahroni	Indonesia	2006-02-09 to 2009-02-07	80	2	Security Gossiper&Bugs Hunter	N/A

Algarni was able to contact most of them to get responses to our questions.

Note: **Hacking** (vulnerability exploitation) does not much skill.
Discovering new (0day) vulnerability takes considerable skill.

A. M. Algarni, and Y. K. Malaiya, "Most Successful Vulnerability Discoverers: Motivation and Methods", Int. Conference on Security and Management (SAM 2013), Las Vegas, July 2013, pp. 3-9.

What happened to discoverers?



Q. Is it illegal to discover New vulnerabilities?

Most of the top discoverers here are credited with discovering the vulnerabilities during the first three years. However, a few discoverers have continued to discover vulnerabilities for several years.

Why do some very successful discoverers disappear from the scene after two to three years?

- A possible explanation is that, during those two to three years, they acquire the notoriety of being accomplished vulnerability discoverers.
- After that, they start offering their services to software developers or security service companies on a contract basis or as employees.
- Some of them may be able to start their own small organizations.

2011-2026: **Most Prolific Vulnerability Discoverers**

Based on historical CVE tracking metrics and platform leaderboards dbugs.

Researcher	Organization / Affiliation	Vulnerabilities Discovered (CVEs)	Country / Location
Abdi Pranata	Independent Researcher	456	Indonesia
John Zuccato	IBM X-Force Ethical Hacking Team	436	United States
Luigi Auriemma	ReSecurity / Independent	430	Malta / Italy
Muhammad Yudha	Independent White-Hat	421	Indonesia
Chris Shepherd	IBM X-Force Ethical Hacking Team	420	United States
Rodney Ryan	IBM X-Force Ethical Hacking Team	416	United States
Rafael Pedrero	Independent	386	Spain
Tran Nguyen Bao Khanh	VNPT Cyber Immunity (VCI)	366	Vietnam
Stealthcopter	Independent	352	United Kingdom
Yuki Chen	Qihoo 360 Vulcan Team	348	China

Major Bug Bounty Platforms

- **HackerOne**: The largest general crowdsourced platform, nearly 2,000 active programs. Serving tech giants, financial institutions, and government agencies like the US Department of Defense.
- **Bugcrowd**: Second largest providing Managed Bug Bounties, Vulnerability Disclosure Programs (VDPs), and Pen-Testing-as-a-Service.
- **Immunefi**: The crowdsourced platform specifically for Web3, smart contracts, and decentralized finance (DeFi).
- **In-House Corporate Programs**: Google VRP, Microsoft, Apple, Meta, etc—often bypass third-party platforms to run massive independent crowdsourced initiatives directly

Crowdsourced bug bounty programs

Invite independent security researchers to legally test an organization's systems for vulnerabilities and paying cash rewards for valid, verified security flaws.

- **Defining the Scope**: The organization partners with a platform to set rules on what apps, domains, or hardware hackers are allowed to test.
- **Testing**: Global ethical hackers use specialized tools and/or manual techniques to probe these for unknown security weaknesses.
- **Submitting a Report**: a researcher submits a secure report detailing how the vulnerability works and providing steps to reproduce it.
- **Verification and severity**: Internal security experts review the submission, verify if it is a real threat, and assign a severity score.
- **Fixing and Rewarding**: The company repairs the code or system configuration, and the researcher receives a financial payout based on the severity of the flaw.

Vulnerability finders



Participants in bug bounty programs
2021 Ultimate Guide to Bug Bounty BugCrowd

Colorado State University

Demographics

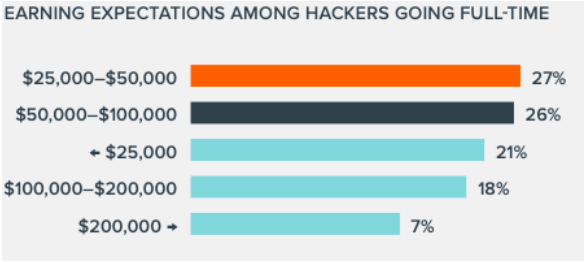
AVERAGE AGE OF HACKERS



HOW HACKERS LEARN SKILLS



68%
of hackers are college graduates.



[INSIDE THE MIND OF A HACKER 2023]

Colorado State University

Classification of Vulnerabilities

OWASP Top Ten

Open Web Application Security Project a nonprofit that works to improve the security of software

A01:2025 - Broken Access Control

A02:2025 - Security Misconfiguration

A03:2025 - Software Supply Chain Failures

A04:2025 - Cryptographic Failures

A05:2025 - Injection

A06:2025 - Insecure Design

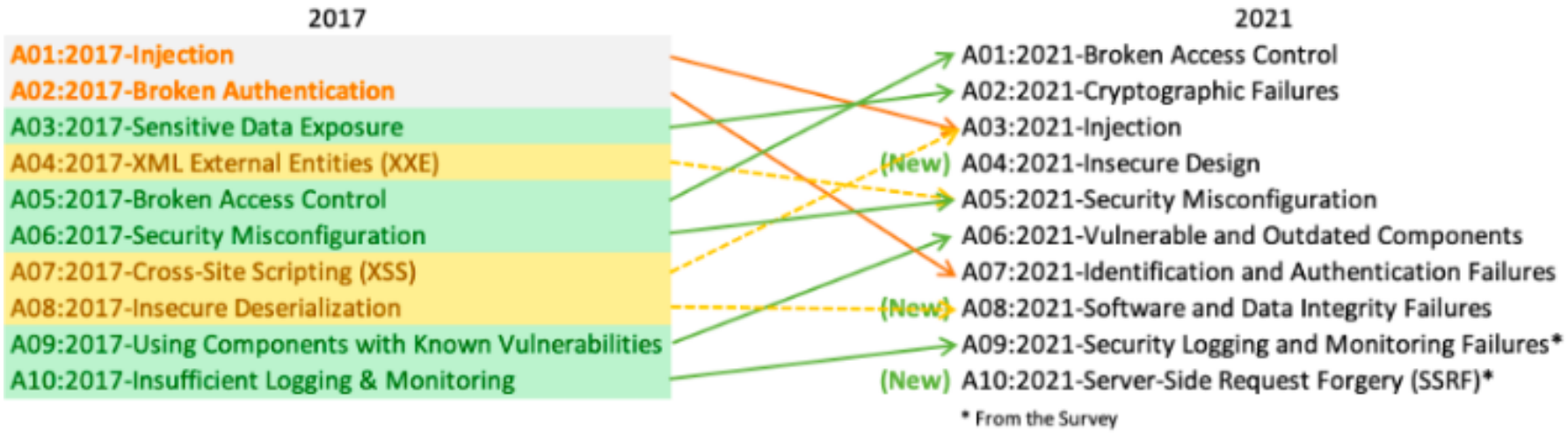
A07:2025 - Authentication Failures

A08:2025 - Software or Data Integrity Failures

A09:2025 - Security Logging and Alerting Failures

A10:2025 - Mishandling of Exceptional Conditions

OWASP Top 10 changes



- Insecure Design: A new category for 2021 focuses on risks related to design and architectural flaws
- Software and Data Integrity Failures: making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity
- Server-Side Request Forgery (SSRF): a web application is fetching a remote resource without validating the user-supplied URL

Vulnerability Classification CVE Details

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2016	418	1096	85	476	90	4	85	39	15	28	0
2017	945	1340	485	1427	252	13	326	101	55	69	1
2018	2055	1720	503	2039	569	111	479	187	118	85	1204
2019	1194	1975	544	2387	485	125	558	136	103	121	878
2020	1212	1818	462	2196	434	107	414	119	130	99	786
2021	1641	2454	740	2713	545	86	520	126	187	133	645
2022	1749	2794	1760	3362	680	85	766	123	228	137	646
2023	1588	1964	2111	5090	736	105	1389	124	237	163	507
2024	1719	2353	2647	7431	911	244	1428	110	372	112	86
2025	2249	2894	3946	8728	1053	672	1950	115	558	166	0
2026	3715	4423	3210	5829	1800	624	1037	120	1424	219	0
Total	18485	24831	16493	41678	7555	2176	8952	1300	3427	1332	4753

https://www.cvedetails.com/vulnerabilities-by-types.php
2016-2026
Note: A vulnerability can have multiple types.

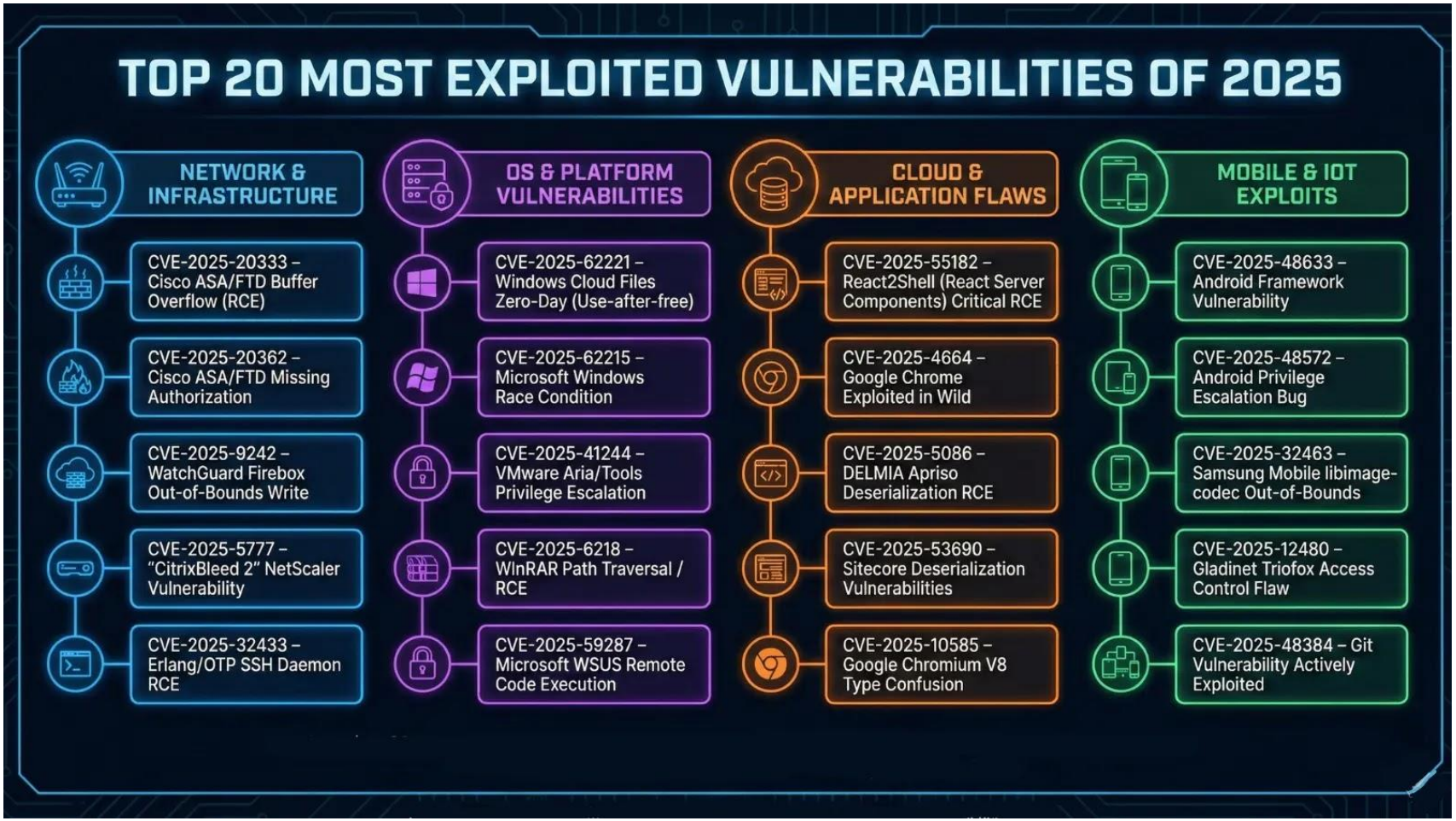
Classification by impact

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2016	1239	1	149	2050	102
2017	1870	340	538	3372	470
2018	1728	640	824	2207	1390
2019	1556	651	895	1697	1313
2020	1695	789	1360	1677	1083
2021	2087	764	1077	2297	906
2022	2067	808	1391	2437	1101
2023	2580	809	1276	2560	1378
2024	3962	628	1052	2470	892
2025	3039	637	1019	2526	742
2026	4834	1850	1447	5324	1168
Total	26657	7917	11028	28617	10545

Vulnerabilities that lead to a denial of service condition published in 2023

)

Top 20 software flaws used by crooks



https://cybersecuritynews.com/most-exploited-vulnerabilities-of-2025/

CVE numbering system

CVE, (Common Vulnerabilities and Exposures), is a list of publicly disclosed computer security flaws.

- A CVE, usually means the CVE ID number assigned to a security flaw ("vulnerability").
- Security advisories issued almost always mention at least one CVE ID.
- CVE is overseen by the MITRE corporation
  - funded from the Cybersecurity and Infrastructure Security Agency, part of the U.S. Department of Homeland Security
- CVE identifiers are assigned by a CVE Numbering Authority (CNA).
  - There are about 100 CNAs, including major IT vendors as well as security companies and research organizations. MITRE can also issue CVEs directly.
  - CVE reports can come from a vendor, a researcher, or anyone who has discovered a flaw
  - There are mechanisms for responsible disclosure.
  - a CVE ID is assigned before a security advisory is made public. Vendors generally keep security flaws secret until a fix has been developed and tested.
  - Once made public, a CVE entry includes
    - the CVE ID (in the format "CVE-2019-1234567"),
    - a brief description of the security vulnerability or exposure, and
    - references, which can include links to vulnerability reports and advisories.

Is it a vulnerability?

CNAs have the discretion to determine whether something is a vulnerability. https://cve.mitre.org/cve/cna/rules.html#section_7-1_what_is_a_vulnerability

- Root CNAs may provide additional guidance to their child CNAs. This allows the program to adapt to definitions used in different industries, legal regimes, and cultures.
  - If a product owner considers an issue to be a vulnerability in its product, then the issue MUST be considered a vulnerability, regardless of whether other parties (e.g., other vendors whose products share the affected code) agree.
  - If the CNA determines that an issue violates the security policy of a product, then the issue SHOULD be considered a vulnerability.
  - If a CNA receives a report about a new vulnerability that has a negative impact, then the reported vulnerability MAY be considered a vulnerability.
- If a *weakness* cannot be exploited by an attacker, it is a weakness, not a *vulnerability*. CWE stands for *Common Weakness Enumeration*.

Responsible Disclosure

A vulnerability discoverer may

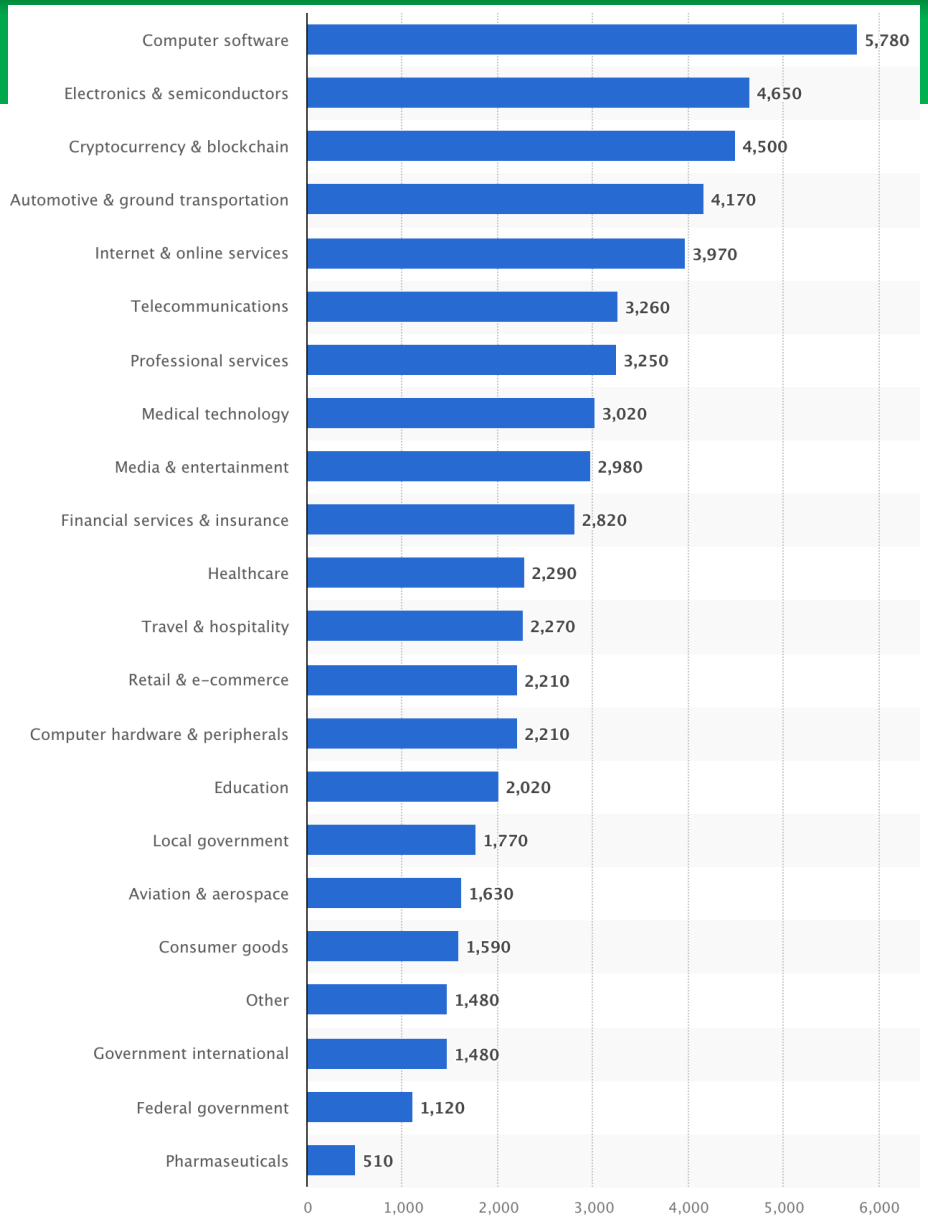
- Submit a report to the company with a Vulnerability Disclosure Program
  - If they have a disclosure program, they will acknowledge the report.
  - Evaluate the report to see if the report is valid.
  - Provide a reward if they have a Reward Program
  - If they do no respond within a fixed time (90-120 days), the discoverer may disclose the vulnerability.
- Sell it to a vulnerability broker (TrendMicro ZDI, HackerOne etc.)
- Sell it to a government organization
- Sell it in the black market (is that legal?)

Reward Programs 2026

Payer / Platform Type	Low Severity Tier	High / Critical Severity Tier	Maximum Ceiling Reward	Key Comments & Specializations
Sherlock (Web3)	$500 – $1,000	$20,000 – $150,000	$16,000,000	Uses a stake-to-submit model. Recorded the largest single payout in tech history for the Usual protocol.
Immunefi (Web3)	$1,000 – $2,500	$50,000 – $1,000,000	$10,000,000	Dedicated exclusively to smart contracts and DeFi. Sky (formerly MakerDAO) maintains a current $10M max bounty.
Apple (In-House Tech)	$5,000 – $10,000	$100,000 – $500,000	$2,000,000+	Focuses heavily on mobile OS and firmware. Max reward scales past $5,000,000 with specific beta/Lockdown Mode bonuses.
Google (In-House Tech)	$500 – $1,500	$30,000 – $250,000	$1,500,000	Covers Android, Chrome, and Core Infrastructure. The $1.5M ceiling is reserved for full-chain compromise of the Pixel Titan M2 chip.
Microsoft (In-House Tech)	$500 – $2,000	$20,000 – $100,000	$250,000	Distributes more total cash than almost any individual program (over $20 million paid out across 15 bounty tracks).
HackerOne (Enterprise Platform)	$50 – $300	$2,000 – $20,000	$2,000,000	The overall market leader. While corporate program averages sit around $15,000 for critical bugs, elite programs (like) scale to $2M.
Bugcrowd (Enterprise Platform)	$50 – $250	$1,500 – $15,000	$100,000+	Focuses on managed testing, VDPs, and pen-testing. Offers highly structured reward metrics based on precise technical risk mapping.
Synack (Premium Platform)	$100 – $500	$5,000 – $50,000	$200,000	A gated, invite-only "Red Team" model. Features a higher baseline payout per bug due to rigorous researcher vetting.

33

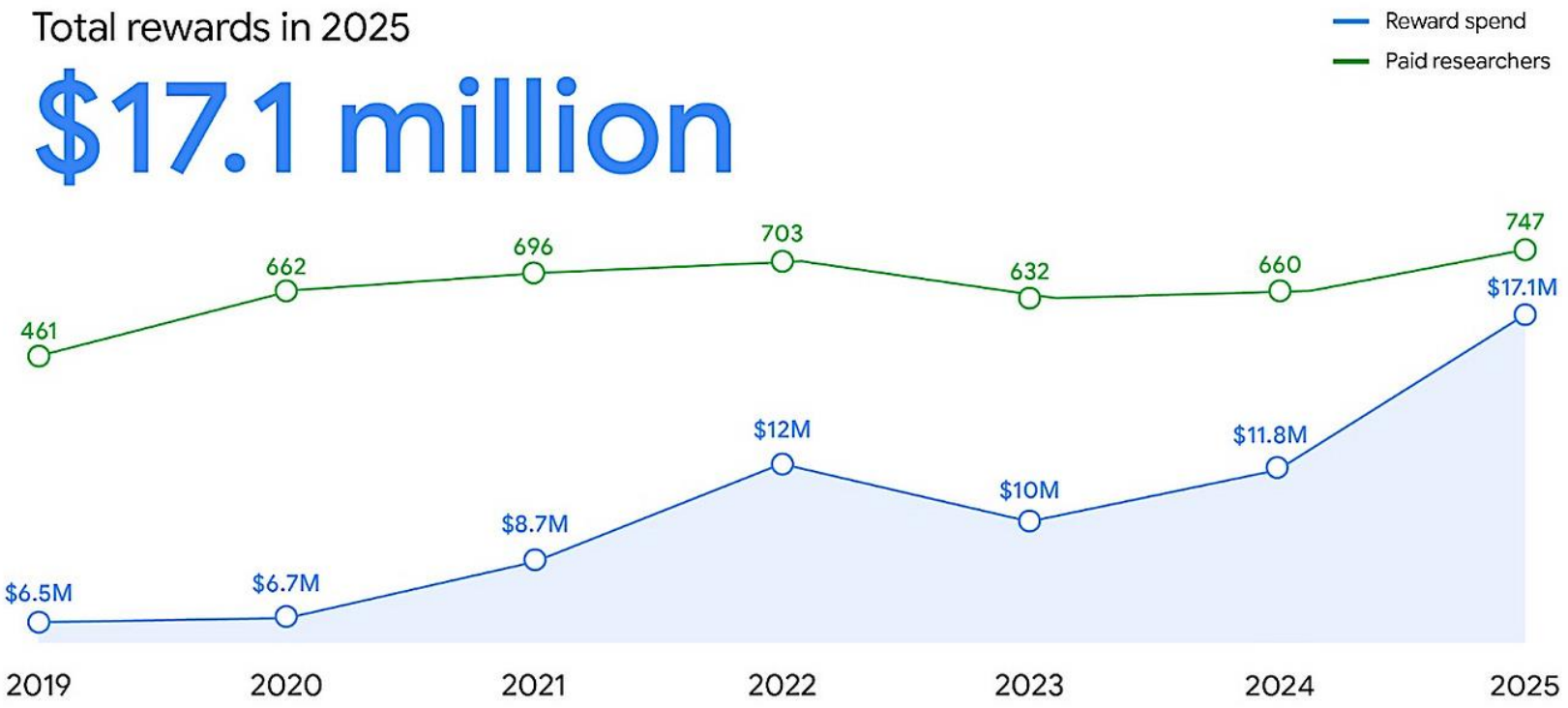
Average Bug Bounty



Average bounty paid for critical vulnerabilities worldwide in 2020, by industry
https://www.statista.com/statistics/1051995/worldwide-bounty-critical-vulnerability/

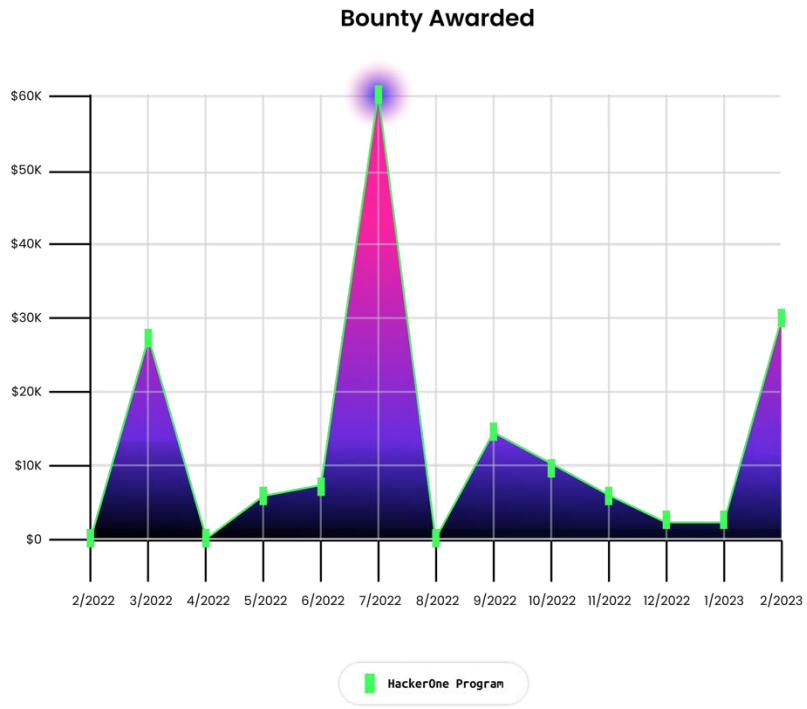
Colorado State University

Google Rewards



Colorado State University

Hacker1



Average Response Time	21 hrs
Average Triage Time	2 days
Average Bounty Time	9 days
Average Resolution Time	1 month

Colorado State University

HackerOne Millionaire



..As if Pereira's story isn't enough, we have to mention another 19-year-old South American who is killing the bug bounty game: Argentina's Santiago Lopez, the first person to top $1 million in earnings on HackerOne's platform.

The self-taught hacker says he got his start by watching YouTube videos and reading blogs on his own, but the thing that jumpstarted his interest in hacking? What else? The 1995 movie Hackers. (Photo by United Artists/Getty Images)

https://www.pcmag.com/news/7-huge-bug-bounty-payouts

CVE numbering system

CVE, (Common Vulnerabilities and Exposures), is a list of publicly disclosed computer security flaws.

- A CVE, usually means the CVE ID number assigned to a security flaw ("vulnerability").
- Security advisories issued almost always mention at least one CVE ID.
- CVE is overseen by the MITRE corporation
  - funded from the Cybersecurity and Infrastructure Security Agency, part of the U.S. Department of Homeland Security
- CVE identifiers are assigned by a CVE Numbering Authority (CNA).
  - There are about 100 CNAs, including major IT vendors as well as security companies and research organizations. MITRE can also issue CVEs directly.
  - CVE reports can come from a vendor, a researcher, or anyone who has discovered a flaw
  - There are mechanisms for responsible disclosure.
  - a CVE ID is assigned before a security advisory is made public. Vendors generally keep security flaws secret until a fix has been developed and tested.
  - Once made public, a CVE entry includes
    - the CVE ID (in the format "CVE-2019-1234567"),
    - a brief description of the security vulnerability or exposure, and
    - references, which can include links to vulnerability reports and advisories.

Vulnerabilities for sale

- Stefan Frei, NSS Labs looked at reports about some of those private vendors
  - Endgame Systems, Exodus Intelligence, Netragard, ReVuln and VUPEN
  - concluded that jointly these firms alone have the capacity to sell more than 100 zero-day exploits per year.

Provider	Offering	Remark / Source
Endgame Systems	25 exploits/year USD $2.5 million	*Business Week* http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html
Exodus Intelligence	60 exploits/year	Service Offering https://www.exodusintel.com/rsrc/ExodusIntelligence_EXP.pdf
ReVuln	> 9 exploits/year	Minimum estimate by counting exploits demonstrated here: http://vimeo.com/53806381 (2013-09-27)
VUPEN	> 7 exploits/year > 15 to 20 binary analysis and private 1-day exploits/month	Minimum estimate by counting list of published exploits here: http://www.vupen.com/blog/ (2013-09-27) Service Offering: http://www.vupen.com/english/services/ba-gov.php

Frei's minimum estimate of exploits offered by boutique exploit providers each year.

https://krebsonsecurity.com/2013/12/how-many-zero-days-hit-you-today/

Vulnerability Data Bases

- Vulnerabilities are security related defects.
- For ordinary defects found, the developers do not have an obligation to report them.
  - They just have to address them in the next patch/version.
- All recognized vulnerabilities are analyzed and reported in the data-bases.
- The new entries in the data-bases are used by antivirus developers/maintainers to add to their signatures.
- Used by researchers like us.

Major vulnerability databases

- NVD National Vulnerability Database https://nvd.nist.gov/
  - US 2005, includes vulnerability operation, its CVSS rating, and links to any available patches/fixes
- CVE Mitre DB https://cve.mitre.org/data/downloads/index.html
- CWE Common weakness enumeration https://cwe.mitre.org/
- VulnDB https://vulndb.cyberriskanalytics.com
  - Open source vulnerability database 2004. Commercia.
- WhiteSource Vuln DB https://www.whitesourcesoftware.com/vulnerability-database/
  - Includes not yet recognized vulnerabilities
- CVEDetails https://www.cvedetails.com better interface?
- Exploit DB https://www.exploit-db.com available exploits

Example: CVE-2018-8174

A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory

- Microsoft acknowledgements
- CVE Details cvss2.0, products/versions affected, links
- Exploit-db has an exploit

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
Vulnerability Life Cycle



CSU Cybersecurity Center
Computer Science Dept