github.com/0xjet/ccc

Crime, Conflicts and Espionage in Cyberspace

The Vulnerability and Exploit Markets

Juan Tapiador (@0xjet)

uc3m

Vulnerabilities

NIST definitions

“A security weakness in a computer.”

“Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source”

“An error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur”

“A condition that enables a threat event to occur.”

“A bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability”

“A weakness in system security procedures, hardware, design, implementation, internal controls, technical controls, physical controls, or other controls that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.”

CVE

Common Vulnerabilities and Exposures

20+ year-old reference method for indexing and describing vulns

CVE record

Descriptive data about a vuln:

- CVE ID (provided by a **CNA**): CVE-YYYY-DDDD
- Description
- At least one public reference
- Data could be enriched by **ADP**s

CVE record states

Reserved | Published | Rejected

CNA

CVE Numbering Authority

Org responsible for:

- Regularly assign CVE IDs to vulns
- Create and publish vuln info in the CVE record

Each CNA has a **scope** of responsibility (set of sw, hw, services)

ADP

Authorized Data Publisher

Org authorized to enrich an existing CVE Record with additional related information (e.g., risk scores, affected product lists, and versions)

CVE-ID

CVE-2021-0001

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Observable timing discrepancy in Intel(R) IPP before version 2020 update 1 may allow authorized user to potentially enable information disclosure via local access.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00477.html
- URL:https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00477.html

Assigning CNA

Intel Corporation

Date Record Created

20201022

Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20201022)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

CVE-ID

CVE-2021-1234

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Assigning CNA

N/A

Date Record Created

20201113

Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20201113)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

A tour to the cve.mitre.org website

Check out the National Vulnerability Database (NVD). Two important enumerations:

- CPE - https://nvd.nist.gov/products/cpe
- CWE - https://cwe.mitre.org

Vulnerability Scoring

Common Vulnerability Scoring System

www.first.org/cvss

Do this online training course for CVSS 3.1 by FIRST (2h)

Mastering CVSS 3.1

Extra activity

20+ years of vulnerability numbering

Explore vulns by

- Date
- Type
- Vendor

Analyze time evolution

Zero-day vulnerabilities

Zero-day vuln	Undisclosed vulnerability Sometimes known but no patch available
N-day vuln	Vuln that is publicly known May or may not have a security patch available
Exploit	Working piece of software that exploits a vuln to achieve some goal, e.g.: LPE RCE DoS SBX VME
(0|N)-day attack	Exploits a (0|N)-day vuln

Three words about exploits

“A room without books is like a body without a soul”
-- Marcus Tullius Cicero

- PoC || GTFO
- The road from a vuln to a working exploit isn’t always easy
- Lots of sources supplying exploits for well-known vulns:

Exploit DB	Packet Storm Exploit Files
Rapid7 V&E DB	Vulnerability Lab
CXSecurity	0day Today

Zero-day misconceptions

Common understanding

Two types of vulnerabilities

Public

- Known to the vendor
- Patch available
- No longer a risk

Private

- Known just by you
- Unpatched
- Used for offensive purposes exclusively

Real world

Richer, more complex situation

Public

- Unfixed or unpatched
- Fixed but not widely patched
- Completely patched
- Immortal

Private

- Known just by 1 who want it secret
- Known by N who want it secret
- Patched but not disclosed

0days in the wild

Explore Google P0's 0day in the wild

The Rise of an Industry

Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER & READY

VRTX

Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

"In 1983, a Silicon Valley startup called Hunter & Ready offered a Volkswagen Beetle as a reward to anyone who could find a "bug" in the firm's Versatile Real-Time Executive (VRTX) operating system."

ACM News, "*Bounties Mount for Bugs*"
Paul Marks, August 23, 2018

Vista Zero-Day Exploit For Sale

Posted by kdawson on Saturday December 16, 2006 @05:02PM from the crack-bazaar dept.

233

Snakepit Bit writes

> "Underground hackers are hawking a zero-day exploit for Windows Vista at $50,000 a pop, according to computer security researchers at Trend Micro. The Windows Vista exploit, which has not been independently verified, was just one of many zero-days available for sale at an auction-style marketplace infiltrated by the anti-virus vendor. Prices for exploits for unpatched code execution flaws are in the $20,000 to $30,000 range. Bots and Trojan downloaders that typically hijack Windows machines for use in botnets were being sold for about $5,000."

From the article:

> "According to [Trend Micro CTO Raimund] Genes, the typical price of a destructive exploit has increased dramatically, driving an underground market that could exceed the value of the legitimate security software business. 'I think the malware industry is making more money than the anti-malware industry,' Genes said."

Security company launches eBay for bugs

Startup offers marketplace where details on unpatched software flaws can be bought and sold

By Robert McMillan
IDG News Service JUL 6, 2007 5:43 AM PST

Psst. Want to buy a zero-day? A Swiss startup called WabiSabiLabi has some for sale, but to qualified buyers only.

V&E as commodities

Vulnerabilities and exploits are atypical information goods

Once exposed, the vendor could patch the vuln and their value decreases

Time-sensitive: vuln can disappear after unintentional patch

When used they might be exposed, decreasing their value

The rise of an industry

Defensive - Bug bounty programs

Google's bounty program: paid out more than US$15M since 2010
Facebook's: US$7.5M since 2011
Microsoft: US$2M paid out in 2018 alone

Offensive - Cyber-arms

Markets surrounding the sale of tools for perpetrating cyberattacks, including software exploits, surveillance technologies, etc.

Stakeholders and the supply chain

Choose your own adventure

Researcher

Defensive Broker

Offensive Broker

Defensive marketplace

Shadow/black marketplace

Software vendor

LEA

Military

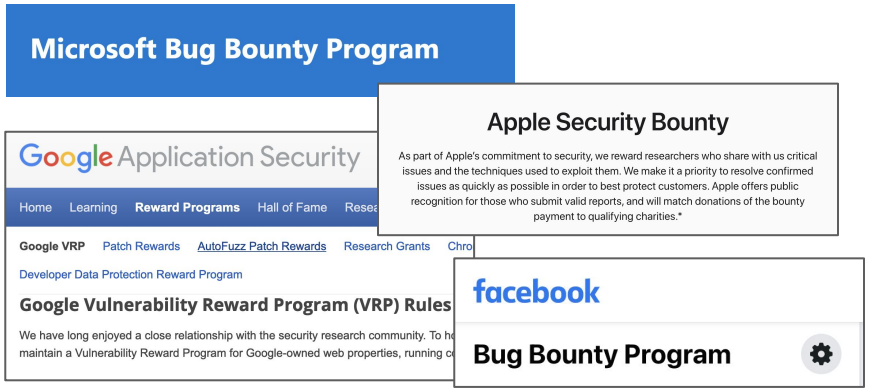
Intel

4hire

Bug bounty programs

Internal programs

Run by the company themselves



Third-party programs

Managed by intermediaries

- Brokers vs marketplaces
- Clandestine vs for-profit business

hackerone

bugcrowd

ZERO DAY INITIATIVE

Walkthroughs

Our Exploit Acquisition Program

PRICE TABLE

INTEGRATED CIRCUITS	
Smart Cards	$100,000+
Cellular SoC (MTK, Qualcomm)	$50,000+
CPLD/FPGA	$50,000+
Microcontrollers	$30,000+

SCADA PLC	
Siemens	$30,000+
Honeywell	$20,000+
Mitsubishi	$15,000+
Omron	$10,000+
ABB	$10,000+
Schneider	$10,000+
Other	$5,000+

ATM	
Wincor	$25,000+
NCR	$25,000+
Diebold	$15,000+
Other	$15,000+

SMART TV	
Samsung	$10,000+
Sony	$10,000+
Panasonic	$10,000+
LG	$5,000+
Home Appliance	$5,000+

NETWORK DEVICES	
Juniper	$50,000+
Cisco	$50,000+
Sonicwall	$50,000+
F5	$50,000+
SIP Avaya, Asterisk, Polycom and others	$50,000+
Riverbed	$50,000+
HP	$10,000+
Huawei	$10,000+
Asus	$5,000+
ZyXEL	$5,000+
Netgear	$5,000+
D-Link	$5,000+
Other	$1,000+

Disclosure often gets thorny

The list of cases is endless

Catalin Cimpanu
@campuscodi

Researcher dumps three iOS zero-days after Apple failed to fix issues for months

therecord.media/researcher-dum...

1:56 PM · Sep 24, 2021 · Twitter Web App

83 Retweets **4** Quote Tweets **214** Likes

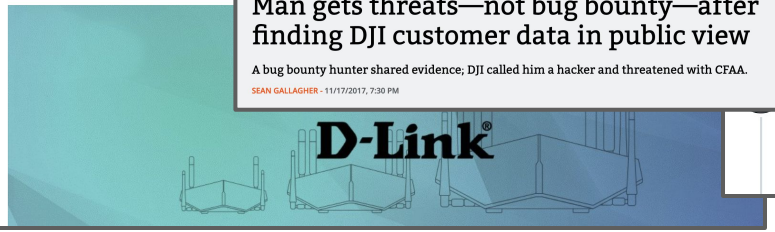
Kosta Eleftheriou
@keleftheriou

Apple ignored this person. Now they're publishing multiple proofs-of-concepts:

"I've reported four 0-day vulnerabilities this year [...], three of them are still present in [iOS 15.0] and one was fixed in 14.7, but Apple decided to cover it up"🤯

Second Researcher Drops Router Exploit Code After D-Link Mishandles Bug Reports

By **Catalin Cimpanu**



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

DRONE WRECK —

Man gets threats—not bug bounty—after finding DJI customer data in public view

A bug bounty hunter shared evidence; DJI called him a hacker and threatened with CFAA.

SEAN GALLAGHER - 11/17/2017, 7:30 PM

Amit Serper
@0xAmit

1/n Thread: Last thing about the whole Microsoft conundrum because I actually have more pressing issues to deal with: Microsoft's attempt via their PR guy and the MVPs that have been dogpiling on me here and on LinkedIn are missing a point. This issue was known for years

7:39 PM · Sep 23, 2021 · Twitter Web App

30 Retweets **4** Quote Tweets **186** Likes

Amit Serper @0xAmit · Sep 23
Replying to @0xAmit
2/n Microsoft had plenty of time to fix or address this issue, either by patching products are just buying all of the autodiscover TLDs (which they are doing right now). Coming after me personally is disgusting and rather shocking to be honest

2 3 73

Amit Serper @0xAmit · Sep 23
3/n Especially when there are research papers, blackhat talks, and news articles that are proving that these issues were known. With that being said, in about 40 minutes I have a meeting with MSRC, hopefully a productive one and I'll share anything that I can with them

2 2 51

Amit Serper @0xAmit · Sep 23
4/n Our blogpost had viable mitigation suggestions in it, which can be implemented fairly quickly and can help to significantly remove the risk of exposure right now. Now, after almost 7 years, Microsoft are taking these issues seriously, buying domains and hopefully fixing

2 36

Walkthrough 1

Walkthrough 2

Protect yourself from legal issues

ELECTRONIC FRONTIER FOUNDATION

Coders' Rights Project

Analysis

The life of zero-days and their exploits

Zero Days, Thousands of Nights

The Life and Times of Zero-Day Vulnerabilities and Their Exploits

Lillian Ablon, Andy Bogart

RAND CORPORATION

Analysis of a dataset of 200 0day exploits and the associated vulns spanning 14 years (2002-2016)

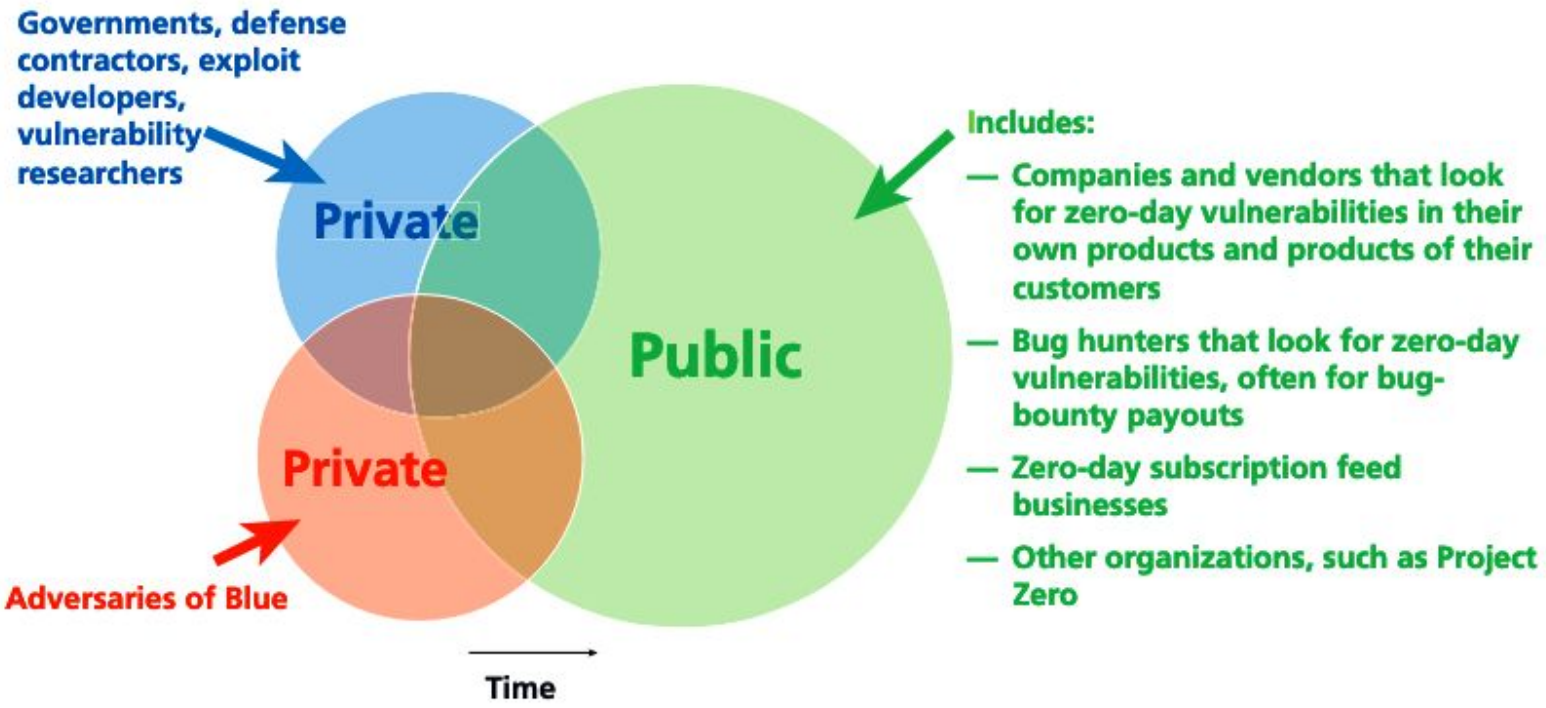
Research questions

1. **Life status:** Is the vulnerability really a zero-day? Is it "alive" (publicly unknown) or "dead" (known to others)?
2. **Longevity:** How long will the vulnerability remain undiscovered and undisclosed to the public?
3. **Collision rate:** What is the likelihood that others will discover and disclose the vulnerability (including other private researchers and the affected vendor)?[12]

It may be additionally helpful to know:

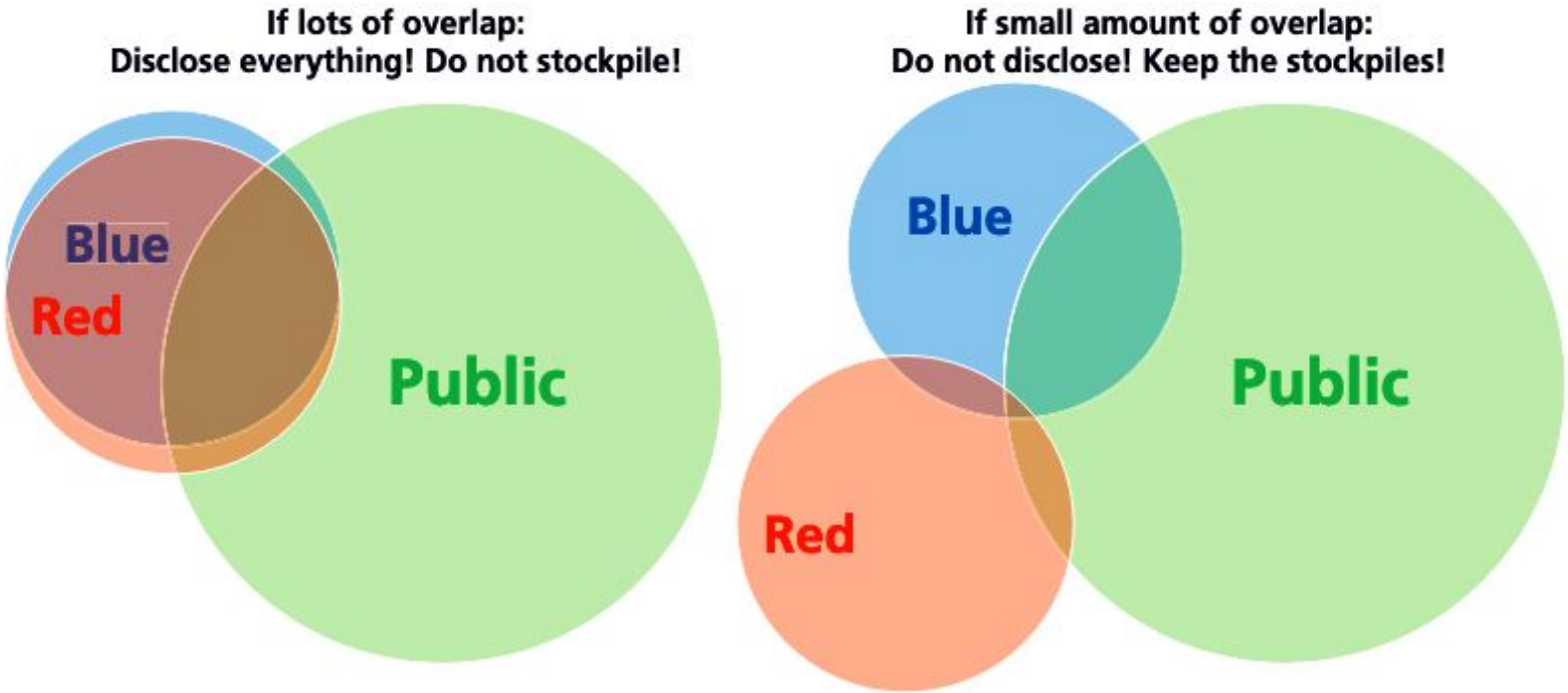
4. **Cost:** What is the cost to develop an exploit for the vulnerability (e.g., in order to help set purchase price)?

Vulnerability inventory



Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.

To stockpile or not to stockpile



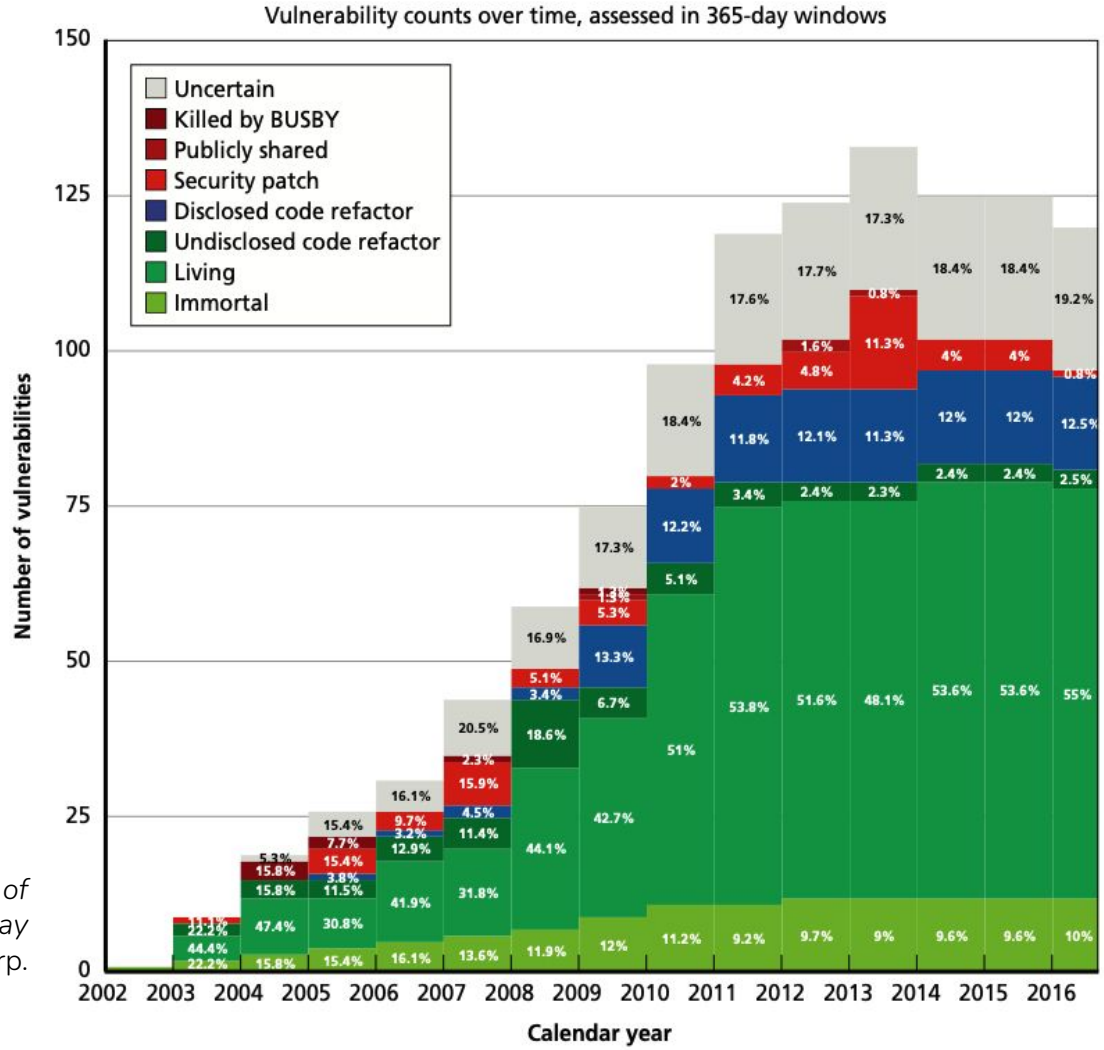
Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.

Life statuses of a vulnerability

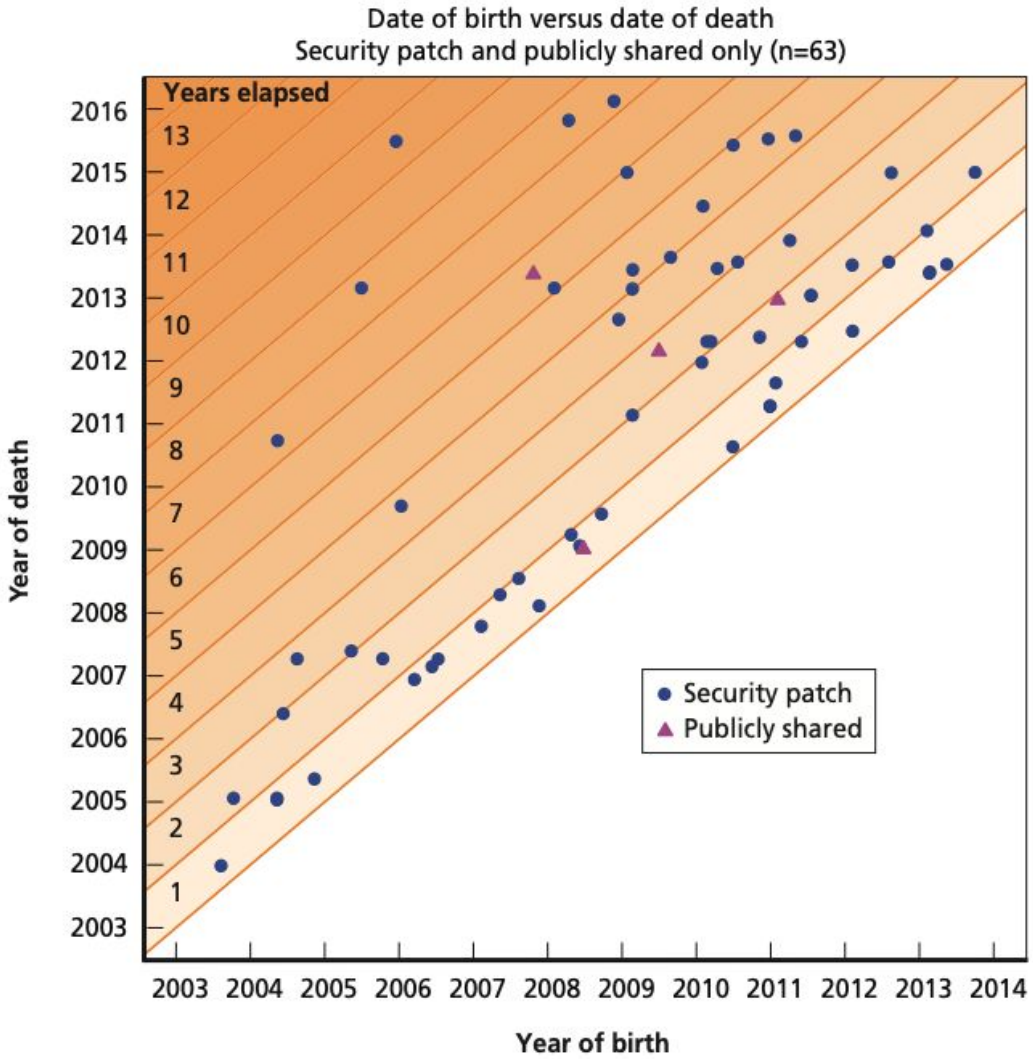
Life Status	Description
Living	A publicly unknown vulnerability for current versions of the product; not found and publicly noted by anyone else (as far as it is known); those in defensive roles are likely actively looking for it.
Immortal	A publicly unknown vulnerability for the version of the product it was created for; that product is no longer maintained (so a security patch will never be issued).
Security Patch	A vulnerability found by a third party and recognized as a security vulnerability; an advisory, patch, and/or CVE has been issued.
Killed by BUSBY	A vulnerability publicly disclosed by the private entity that found it when they realized that vulnerability was about to be found, or when they wanted to use a particular vulnerability as a teaching tool or for marketing purposes.
Publicly Shared	A vulnerability found by a third party and publicly discussed, but *not* publicly recognized as a security vulnerability; no advisory, patch, and/or CVE issued.
Code Refactor	A likely publicly unknown vulnerability for past versions of a product that is no longer exploitable in current versions due to code revisions; the product is still maintained (so a security patch sometime in the future is still possible for the past versions).

Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.

Status of the stockpile



Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.



Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.

Life expectancy

Finding #1: Declaring a vulnerability as alive (publicly unknown) or dead (publicly known) may be misleading and too simplistic

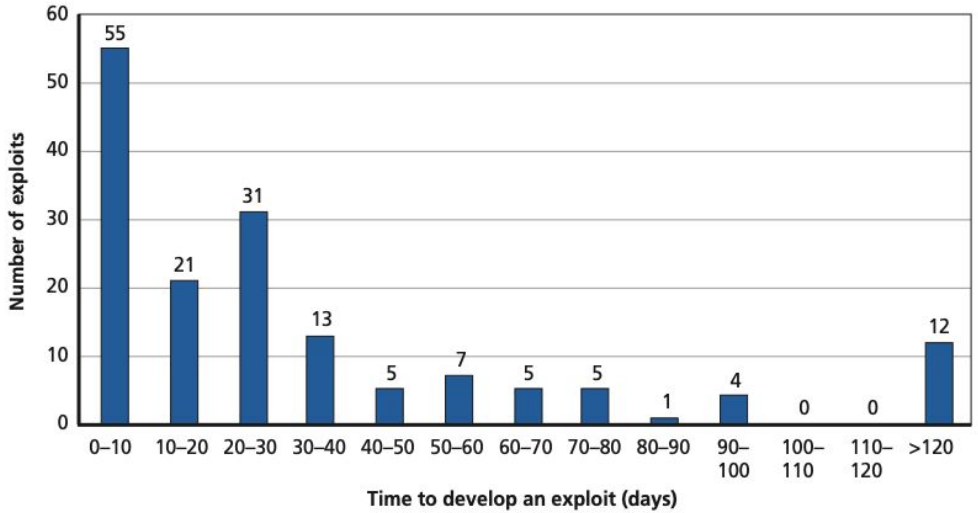
Finding #2: Exploits have an average life expectancy of 6.9 years after initial discovery; but roughly 25 percent of exploits will not survive for more than a year and a half, and another 25 percent will survive more than 9.5 years

Finding #3: No characteristics of a vulnerability indicated a long or short life; however, future analyses may want to examine Linux versus other platform types, the similarity of open and closed source code, and various groupings of exploit class type

Finding #4: For a given stockpile of zero-day vulnerabilities, after a year approximately 5.7 percent have been discovered by others

Exploit development costs

> We found that exploit development time ranges, but is generally relatively short. In our data, 71 percent of the exploits were developed in a month (31 days or less), almost a third (31.44 percent) were developed in a week or less, and only 10 percent took more than 90 days to exploit.[30] The majority of exploits in our dataset took between 6 and 37 days to become fully functional (with a median of 22 days, minimum of 1 day, and maximum of 955 days).



Source: Ablon and Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. RAND Corp.

0days are not your biggest problem

"We found that 99.9 percent of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published."

-- Verizon's 2016 Data Breach Investigations Report

The Ethics of Vuln Research

Ethics != Law

	LEGAL	ILEGAL
GOOD		
EVIL		

Source: D&D fandom.
https://dungeonsdragons.fandom.com/wiki/Alignment

Ethics in vulnerability research and, more broadly, in computer security

What is ethics?

What does ethics have to do with your work?

Computer ethics

ACM Code of Ethics and Professional Conduct

1. GENERAL ETHICAL PRINCIPLES.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

1.2 Avoid harm.

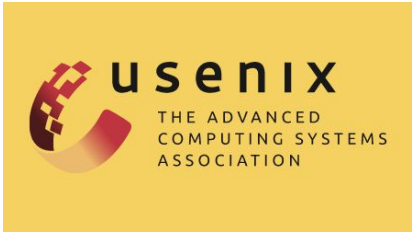
1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.



The System Administrators' Code of Ethics

We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct, and agree to be guided by this code of ethics, and encourage every System Administrator to do the same.

Professionalism I will maintain professional conduct in the workplace and will not allow personal feelings or beliefs to cause me to treat people unfairly or unprofessionally.

Personal Integrity I will be honest in my professional dealings and forthcoming about my competence and the impact of my mistakes. I will seek assistance from others when required.

I will avoid conflicts of interest and biases whenever possible. When my advice is sought, if I have a conflict of interest or bias, I will declare it if appropriate, and recuse myself if necessary.

Privacy I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it.

Laws and Policies I will educate myself and others on relevant laws, regulations, and policies regarding the performance of my duties.

Communication I will communicate with management, users, and colleagues about computer matters of mutual interest. I will strive to listen to and understand the needs of all parties.

System Integrity I will strive to ensure the necessary integrity, reliability, and availability of the systems for which I am responsible.

I will design and maintain each system in a manner to support the purpose of the system to the organization.

Education I will continue to update and enhance my technical knowledge and other work-related skills. I will share my knowledge and experience with others.

Responsibility to Computing Community I will cooperate with the larger computing community to maintain the integrity of network and computing resources.

Social Responsibility As an informed professional, I will encourage the writing and adoption of relevant policies and laws consistent with these ethical principles.

Ethical Responsibility I will strive to build and maintain a safe, healthy, and productive workplace.

I will do my best to make decisions consistent with the safety, privacy, and well-being of my community and the public, and to disclose promptly factors that might pose unexamined risks or dangers.

I will accept and offer honest criticism of technical work as appropriate and will credit properly the contributions of others.

I will lead by example, maintaining a high ethical standard and degree of professionalism in the performance of all my duties. I will support colleagues and co-workers in following this code of ethics.

Ethics in computer security

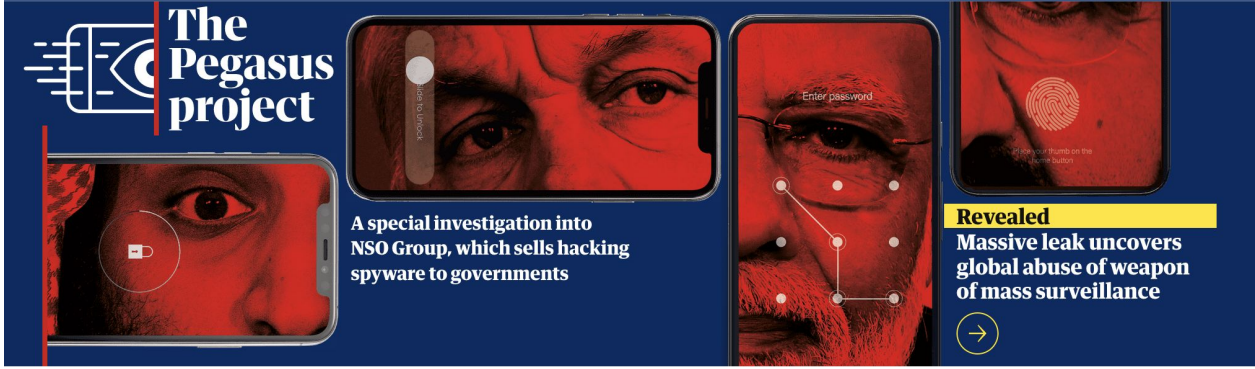
Duty of trustworthiness
Duty of coordinated vulnerability disclosure
Duty of confidentiality
Duty to acknowledge
Duty of authorization
Duty to inform
Duty to respect human rights
Duty to Team health
Duty to Team ability
Duty for responsible collection
Duty to recognize jurisdictional boundaries
Duty of evidence-based reasoning

Possible dilemmas

#1 - Hacking for a Gov (LEA, Intel)

#2 - A dangerous vulnerability

The Guardian



FORCEDENTRY

NSO Group iMessage Zero-Click Exploit Captured in the Wild

By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert

September 13, 2021

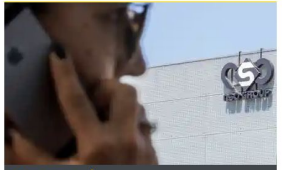
Hungary / Phones of journalist who tracked Viktor Orban's childhood friend infected with spyware

Dániel Németh's phones infected with Pegasus software while reporting on one of Hungary's richest men

EU / Commissioner calls for urgent action against Pegasus spyware

Bahrain / Phones of nine Bahraini activists found to have been hacked with NSO spyware

Princess Latifa / Campaigner had 'phone compromised by Pegasus spyware'



France / Pegasus spyware found on journalists' phones, French intelligence confirms

NSO ownership / Investors in talks to transfer management of fund that owns Israeli spyware company NSO

Project Zero

News and updates from the Project Zero team at Google

Thursday, August 29, 2019

A very deep dive into iOS Exploit chains found in the wild

Posted by Ian Beer, Project Zero

Computing / Cybersecurity

How China turned a prize-winning iPhone hack against the Uyghurs

An attack that targeted Apple devices was used to spy on China's Muslim minority—and US officials claim it was developed at the country's top hacking competition.

by **Patrick Howell O'Neill** May 6, 2021

- Beijing secretly used an award-winning iPhone hack to spy on Uyghurs
- The United States tracked the attack and informed Apple
- Tianfu Cup is a "venue for China to get zero-days," say experts

The NSA can play either defense or offense. It can either alert the vendor and get a still-secret vulnerability fixed, or it can hold on to it and use it as to eavesdrop on foreign computer systems. Both are important U.S. policy goals, but the NSA has to choose which one to pursue. By fixing the vulnerability, it strengthens the security of the Internet against all attackers: other countries, criminals, hackers. By leaving the vulnerability open, it is better able to attack others on the Internet. But each use runs the risk of the target government learning of, and using for itself, the vulnerability—or of the vulnerability becoming public and criminals starting to use it.

Source: Bruce Schneier. *Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?* The Atlantic, May 19, 2014

Heartbleed: Understanding When We Disclose Cyber Vulnerabilities

APRIL 28, 2014 AT 3:00 PM ET BY MICHAEL DANIEL

Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest. But that is not the same as arguing that we should completely forgo this tool as a way to conduct intelligence collection, and better protect our country in the long-run. Weighing these tradeoffs is not easy, and so we have established principles to guide agency decision-making in this area.

We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed. While there are no hard and fast rules, here are a few things I want to know when an agency proposes temporarily withholding knowledge of a vulnerability:

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

New Law Will Help Chinese Government Stockpile Zero-Days

By Kevin Townsend on July 14, 2021

China rules that all zero-day vulnerabilities must be disclosed only to the Chinese Government

Starting September 1, 2021, the Chinese government will require that any Chinese citizen who finds a zero-day vulnerability must pass the details to the Chinese government and must not sell or give the knowledge to any third-party outside of China (apart from the vulnerable product's manufacturer).

In 2013, a mysterious group of hackers that calls itself the Shadow Brokers stole a few disks full of National Security Agency secrets. Since last summer, they've been dumping these secrets on the internet. They have publicly embarrassed the NSA and damaged its intelligence-gathering capabilities, while at the same time have put sophisticated cyberweapons in the hands of anyone who wants them. They have exposed major vulnerabilities in Cisco routers, Microsoft Windows, and Linux mail servers, forcing those companies and their customers to scramble. And they gave the authors of the WannaCry ransomware the exploit they needed to infect hundreds of thousands of computer worldwide this month.

Source: Bruce Schneier. *Who Are the Shadow Brokers?* The Atlantic, May 23, 2017