Project Zero

News and updates from the Project Zero team at Google

Vulnerability Disclosure Policy

90+30 policy

Project Zero follows a 90+30 disclosure deadline policy, which means that a vendor has 90 days after Project Zero notifies them about a security vulnerability to make a patch available to users. If they make a patch available within 90 days, Project Zero will publicly disclose details of the vulnerability 30 days after the patch has been made available to users.

For example:

- If a vendor patches a security issue 47 days after Project Zero notified the vendor about the vulnerability, details would be made public on day 77.
- If a vendor patches a security issue 83 days after Project Zero notified the vendor about the vulnerability, details would be made public on day 113.

If a vendor is unable to patch an issue within the initial 90 days, Project Zero will make the details of the vulnerability public at the end of the 90-day period.

Grace period

If a vendor is unable to make a patch available in 90 days, but will make a patch available within an additional 14 days (i.e., within 104 days since the vulnerability was disclosed to the vendor), Project Zero may grant a grace period to the vendor upon request. In that case, Project Zero will publicly disclose details of the vulnerability 120 days after the vulnerability was initially disclosed to the public.

In-the-wild vulnerabilities

As described in Google's application security vulnerability disclosure policy, if Project Zero finds evidence that a vulnerability is being actively exploited against real users "in the wild", a 7-day disclosure policy replaces the 90-day policy. However, the 30-day window still applies, meaning that Project Zero will publicly release details of the vulnerability 30 days after a patch is made available to users, as long as a patch was made available by the end of the 7-day deadline.

The grace period for in-the-wild vulnerabilities is 3 days. Similar to the 90-day policy, public details for patches made available during the grace period will still be released to the public 30 days after the original deadline (i.e., day 37), regardless of on which day the patch is released.

Mutually-agreed early disclosure

In any of the above cases, Project Zero and the relevant vendor can mutually agree to release details of a vulnerability earlier than the date indicated by policy.

For more information and background on our policy, please see the explainer blog post and our disclosure policy FAQ.

Search This Blog

Search

Pages

- About Project Zero
- Working at Project Zero
- 0day "In the Wild"
- 0day Exploit Root Cause Analyses
- Vulnerability Disclosure FAQ

Archives

2025

- The Windows Registry Adventure #8: Practical explo... (May)
- The Windows Registry Adventure #7: Attack surface ... (May)
- Breaking the Sound Barrier Part I: Fuzzing CoreAud... (May)
- The Windows Registry Adventure #6: Kernel-mode obj... (Apr)
- Blasting Past Webp (Mar)
- Windows Bug Class: Accessing Trapped COM Objects w... (Jan)
- Windows Exploitation Tricks: Trapping Virtual Memo... (Jan)

2024

- The Windows Registry Adventure #5: The regf file f... (Dec)
- The Qualcomm DSP Driver - Unexpectedly Excavating ... (Dec)
- Windows Tooling Updates: OleView.NET (Dec)
- Simple macOS kernel extension fuzzing in userspace... (Nov)
- From Naptime to Big Sleep: Using Large Language Mo... (Oct)
- The Windows Registry Adventure #4: Hives and the r... (Oct)
- Effective Fuzzing: A Dav1d Case Study (Oct)
- The Windows Registry Adventure #3: Learning resources (Jun)
- Project Naptime: Evaluating Offensive Security Cap... (Jun)
- Driving forward in Android drivers (Jun)

No comments:

Post a Comment

Home

Subscribe to: Posts (Atom)

- The Windows Registry Adventure #2: A brief history... (Apr)
- The Windows Registry Adventure #1: Introduction an... (Apr)

2023

- First handset with MTE on the market (Nov)
- An analysis of an in-the-wild iOS Safari WebConten... (Oct)
- Analyzing a Modern In-the-wild Android Exploit (Sep)
- MTE As Implemented, Part 1: Implementation Testing (Aug)
- MTE As Implemented, Part 3: The Kernel (Aug)
- MTE As Implemented, Part 2: Mitigation Case Studies (Aug)
- Summary: MTE As Implemented (Aug)
- Release of a Technical Report into Intel Trust Dom... (Apr)
- Multiple Internet to Baseband Remote Code Executio... (Mar)
- Exploiting null-dereferences in the Linux kernel (Jan)
- DER Entitlements: The (Brief) Return of the Psychi... (Jan)

2022

- Exploiting CVE-2022-42703 - Bringing back the stac... (Dec)
- Mind the Gap (Nov)
- A Very Powerful Clipboard: Analysis of a Samsung i... (Nov)
- Gregor Samsa: Exploiting Java&#39;s XML Signature Veri... (Nov)
- RC4 Is Still Considered Harmful (Oct)
- The quantum state of Linux kernel garbage collecti... (Aug)
- 2022 0-day In-the-Wild Exploitation…so far (Jun)
- The curious tale of a fake Carrier.app (Jun)
- An Autopsy on a Zombie In-the-Wild 0-day (Jun)
- Release of Technical Report into the AMD Security ... (May)
- The More You Know, The More You Know You Don’t Know (Apr)
- CVE-2021-1782, an iOS in-the-wild vulnerability in... (Apr)
- CVE-2021-30737, @xerub&#39;s 2021 iOS ASN.1 Vulnerability (Apr)
- FORCEDENTRY: Sandbox Escape (Mar)
- Racing against the clock -- hitting a tiny kernel ... (Mar)
- A walk through Project Zero metrics (Feb)

- Zooming in on Zero-click Exploits (Jan)

2021

- A deep dive into an NSO zero-click iMessage exploi... (Dec)
- This shouldn&#39;t have happened: A vulnerability post... (Dec)
- Windows Exploitation Tricks: Relaying DCOM Authent... (Oct)
- Using Kerberos for Authentication Relay Attacks (Oct)
- How a simple Linux kernel memory corruption bug ca... (Oct)
- Fuzzing Closed-Source JavaScript Engines with Cove... (Sep)
- Understanding Network Access in Windows AppContainers (Aug)
- An EPYC escape: Case-study of a KVM breakout (Jun)
- Fuzzing iOS code on macOS at native speed (May)
- Designing sockfuzzer, a network syscall fuzzer for... (Apr)
- Policy and Disclosure: 2021 Edition (Apr)
- Who Contains the Containers? (Apr)
- In-the-Wild Series: October 2020 0-day discovery (Mar)
- Déjà vu-lnerability (Feb)
- A Look at iMessage in iOS 14 (Jan)
- Windows Exploitation Tricks: Trapping Virtual Memo... (Jan)
- The State of State Machines (Jan)
- Hunting for Bugs in Windows Mini-Filter Drivers (Jan)
- In-the-Wild Series: Android Exploits (Jan)
- In-the-Wild Series: Android Post-Exploitation (Jan)
- In-the-Wild Series: Windows Exploits (Jan)
- In-the-Wild Series: Chrome Exploits (Jan)
- In-the-Wild Series: Chrome Infinity Bug (Jan)
- Introducing the In-the-Wild Series (Jan)

2020

- An iOS hacker tries Android (Dec)
- An iOS zero-click radio proximity exploit odyssey (Dec)
- Oops, I missed it again! (Nov)
- Enter the Vault: Authentication Issues in HashiCor... (Oct)
- Announcing the Fuzzilli Research Grant Program (Oct)
- Attacking the Qualcomm Adreno GPU (Sep)

- JITSploitation I: A JIT Bug (Sep)
- JITSploitation II: Getting Read/Write (Sep)
- JITSploitation III: Subverting Control Flow (Sep)
- MMS Exploit Part 5: Defeating Android ASLR, Gettin... (Aug)
- Exploiting Android Messengers with WebRTC: Part 3 (Aug)
- Exploiting Android Messengers with WebRTC: Part 2 (Aug)
- MMS Exploit Part 4: MMS Primer, Completing the ASL... (Aug)
- Exploiting Android Messengers with WebRTC: Part 1 (Aug)
- The core of Apple is PPL: Breaking the XNU kernel&#39;... (Jul)
- One Byte to rule them all (Jul)
- Detection Deficit: A Year in Review of 0-days Used... (Jul)
- Root Cause Analyses for 0-day In-the-Wild Exploits (Jul)
- MMS Exploit Part 3: Constructing the Memory Corrup... (Jul)
- MMS Exploit Part 2: Effective Fuzzing of the Qmage... (Jul)
- MMS Exploit Part 1: Introduction to the Samsung Qm... (Jul)
- How to unc0ver a 0-day in 4 hours or less (Jul)
- FF Sandbox Escape (CVE-2020-12388) (Jun)
- A survey of recent iOS kernel exploits (Jun)
- Fuzzing ImageIO (Apr)
- You Won&#39;t Believe what this One Line Change Did to... (Apr)
- TFW you-get-really-excited-you-patch-diffed-a-0day... (Apr)
- Escaping the Chrome Sandbox with RIDL (Feb)
- Mitigations are attack surface, too (Feb)
- A day^W^W Several months in the life of Project Ze... (Feb)
- A day^W^W Several months in the life of Project Ze... (Feb)
- Part II: Returning to Adobe Reader symbols on macOS (Jan)
- Remote iPhone Exploitation Part 2: Bringing Light ... (Jan)
- Remote iPhone Exploitation Part 3: From Memory Cor... (Jan)
- Remote iPhone Exploitation Part 1: Poking Memory v... (Jan)
- Policy and Disclosure: 2020 Edition (Jan)

2019

- Calling Local Windows RPC Servers from .NET (Dec)

- SockPuppet: A Walkthrough of a Kernel Exploit for ... (Dec)
- Bad Binder: Android In-The-Wild Exploit (Nov)
- KTRW: The journey to build a debuggable iPhone (Oct)
- The story of Adobe Reader symbols (Oct)
- Windows Exploitation Tricks: Spoofing Name... (Sep)
- A very deep dive into iOS Exploit chains found in ... (Aug)
- In-the-wild iOS Exploit Chain 1 (Aug)
- In-the-wild iOS Exploit Chain 5 (Aug)
- In-the-wild iOS Exploit Chain 4 (Aug)
- In-the-wild iOS Exploit Chain 3 (Aug)
- In-the-wild iOS Exploit Chain 2 (Aug)
- Implant Teardown (Aug)
- JSC Exploits (Aug)
- The Many Possibilities of CVE-2019-8646 (Aug)
- Down the Rabbit-Hole... (Aug)
- The Fully Remote Attack Surface of the iPhone (Aug)
- Trashing the Flow of Data (May)
- Windows Exploitation Tricks: Abusing the User-Mode... (Apr)
- Virtually Unlimited Memory: Escaping the Chrome Sa... (Apr)
- Splitting atoms in XNU (Apr)
- Windows Kernel Logic Bug Class: Access Mode Mismat... (Mar)
- Android Messaging: A Few Bugs Short of a Chain (Mar)
- The Curious Case of Convexity Confusion (Feb)
- Examining Pointer Authentication on the iPhone XS (Feb)
- voucher_swap: Exploiting MIG reference counting in... (Jan)
- Taking a page from the kernel&#39;s book: A TLB issue ... (Jan)

2018

- On VBScript (Dec)
- Searching statically-linked vulnerable library fun... (Dec)
- Adventures in Video Conferencing Part 5: Where Do ... (Dec)
- Adventures in Video Conferencing Part 4: What Didn... (Dec)
- Adventures in Video Conferencing Part 3: The Even ... (Dec)
- Adventures in Video Conferencing Part 2: Fun with ... (Dec)

- Adventures in Video Conferencing Part 1: The Wild ... (Dec)
- Injecting Code into Windows Protected Processes us... (Nov)
- Heap Feng Shader: Exploiting SwiftShader in Chrome (Oct)
- Deja-XNU (Oct)
- Injecting Code into Windows Protected Processes us... (Oct)
- 365 Days Later: Finding and Exploiting Safari Bugs... (Oct)
- A cache invalidation bug in Linux memory management (Sep)
- OATmeal on the Universal Cereal Bus: Exploiting An... (Sep)
- The Problems and Promise of WebAssembly (Aug)
- Windows Exploitation Tricks: Exploiting Arbitrary ... (Aug)
- Adventures in vulnerability reporting (Aug)
- Drawing Outside the Box: Precision Issues in Graph... (Jul)
- Detecting Kernel Memory Disclosure – Whitepaper (Jun)
- Bypassing Mitigations by Attacking JIT Server in M... (May)
- Windows Exploitation Tricks: Exploiting Arbitrary ... (Apr)
- Reading privileged memory with a side-channel (Jan)

2017

- aPAColypse now: Exploiting Windows 10 in a Local N... (Dec)
- Over The Air - Vol. 2, Pt. 3: Exploiting The Wi-Fi... (Oct)
- Using Binary Diffing to Discover Windows Kernel Me... (Oct)
- Over The Air - Vol. 2, Pt. 2: Exploiting The Wi-Fi... (Oct)
- Over The Air - Vol. 2, Pt. 1: Exploiting The Wi-Fi... (Sep)
- The Great DOM Fuzz-off of 2017 (Sep)
- Bypassing VirtualBox Process Hardening on Windows (Aug)
- Windows Exploitation Tricks: Arbitrary Directory C... (Aug)
- Trust Issues: Exploiting TrustZone TEEs (Jul)
- Exploiting the Linux kernel via packet sockets (May)
- Exploiting .NET Managed DCOM (Apr)
- Exception-oriented exploitation on iOS (Apr)
- Over The Air: Exploiting Broadcom’s Wi-Fi Stack (P... (Apr)
- Notes on Windows Uniscribe Fuzzing (Apr)
- Pandavirtualization: Exploiting the Xen hypervisor (Apr)

- Over The Air: Exploiting Broadcom’s Wi-Fi Stack (P... (Apr)
- Project Zero Prize Conclusion (Mar)
- Attacking the Windows NVIDIA Driver (Feb)
- Lifting the (Hyper) Visor: Bypassing Samsung’s Rea... (Feb)

2016

- Chrome OS exploit: one byte overflow and symlinks (Dec)
- BitUnmap: Attacking Android Ashmem (Dec)
- Breaking the Chain (Nov)
- task_t considered harmful (Oct)
- Announcing the Project Zero Prize (Sep)
- Return to libstagefright: exploiting libutils on A... (Sep)
- A Shadow of our Former Self (Aug)
- A year of Windows kernel font fuzzing #2: the tech... (Jul)
- How to Compromise the Enterprise Endpoint (Jun)
- A year of Windows kernel font fuzzing #1: the results (Jun)
- Exploiting Recursion in the Linux Kernel (Jun)
- Life After the Isolated Heap (Mar)
- Race you to the kernel! (Mar)
- Exploiting a Leaked Thread Handle (Mar)
- The Definitive Guide on Win32 to NT Path Conversion (Feb)
- Racing MIDI messages in Chrome (Feb)
- Raising the Dead (Jan)

2015

- FireEye Exploitation: Project Zero’s Vulnerability... (Dec)
- Between a Rock and a Hard Link (Dec)
- Windows Sandbox Attack Surface Analysis (Nov)
- Hack The Galaxy: Hunting Bugs in the Samsung Galax... (Nov)
- Windows Drivers are True’ly Tricky (Oct)
- Revisiting Apple IPC: (1) Distributed Objects (Sep)
- Kaspersky: Mo Unpackers, Mo Problems. (Sep)
- Stagefrightened? (Sep)
- Enabling QR codes in Internet Explorer, or a story... (Sep)
- Windows 10^H^H Symbolic Link Mitigations (Aug)
- One font vulnerability to rule them all #4: Window... (Aug)

- Three bypasses and a fix for one of Flash&#39;s Vector... (Aug)
- Attacking ECMAScript Engines with Redefinition (Aug)
- One font vulnerability to rule them all #3: Window... (Aug)
- One font vulnerability to rule them all #2: Adobe ... (Aug)
- One font vulnerability to rule them all #1: Introd... (Jul)
- One Perfect Bug: Exploiting Type Confusion in Flash (Jul)
- Significant Flash exploit mitigations are live in ... (Jul)
- From inter to intra: gaining reliability (Jul)
- When ‘int’ is the new ‘short’ (Jul)
- What is a &quot;good&quot; memory corruption vulnerability? (Jun)
- Analysis and Exploitation of an ESET Vulnerability (Jun)
- Owning Internet Printing - A Case Study in Modern ... (Jun)
- Dude, where’s my heap? (Jun)
- In-Console-Able (May)
- A Tale of Two Exploits (Apr)
- Taming the wild copy: Parallel Thread Corruption (Mar)
- Exploiting the DRAM rowhammer bug to gain kernel p... (Mar)
- Feedback and data-driven updates to Google’s discl... (Feb)
- (^Exploiting)\s*(CVE-2015-0318)\s*(in)\s*(Flash$) (Feb)
- A Token’s Tale (Feb)
- Exploiting NVMAP to escape the Chrome sandbox - CV... (Jan)
- Finding and exploiting ntpd vulnerabilities (Jan)

2014

- Internet Explorer EPM Sandbox Escape CVE-2014-6350 (Dec)
- pwn4fun Spring 2014 - Safari - Part II (Nov)
- Project Zero Patch Tuesday roundup, November 2014 (Nov)
- Did the “Man With No Name” Feel Insecure? (Oct)
- More Mac OS X and iPhone sandbox escapes and kerne... (Oct)
- Exploiting CVE-2014-0556 in Flash (Sep)
- The poisoned NUL byte, 2014 edition (Aug)
- What does a pointer look like, anyway? (Aug)
- Mac OS X and iPhone sandbox escapes (Jul)
- pwn4fun Spring 2014 - Safari - Part I (Jul)

- Announcing Project Zero (Jul)