theori | Blog

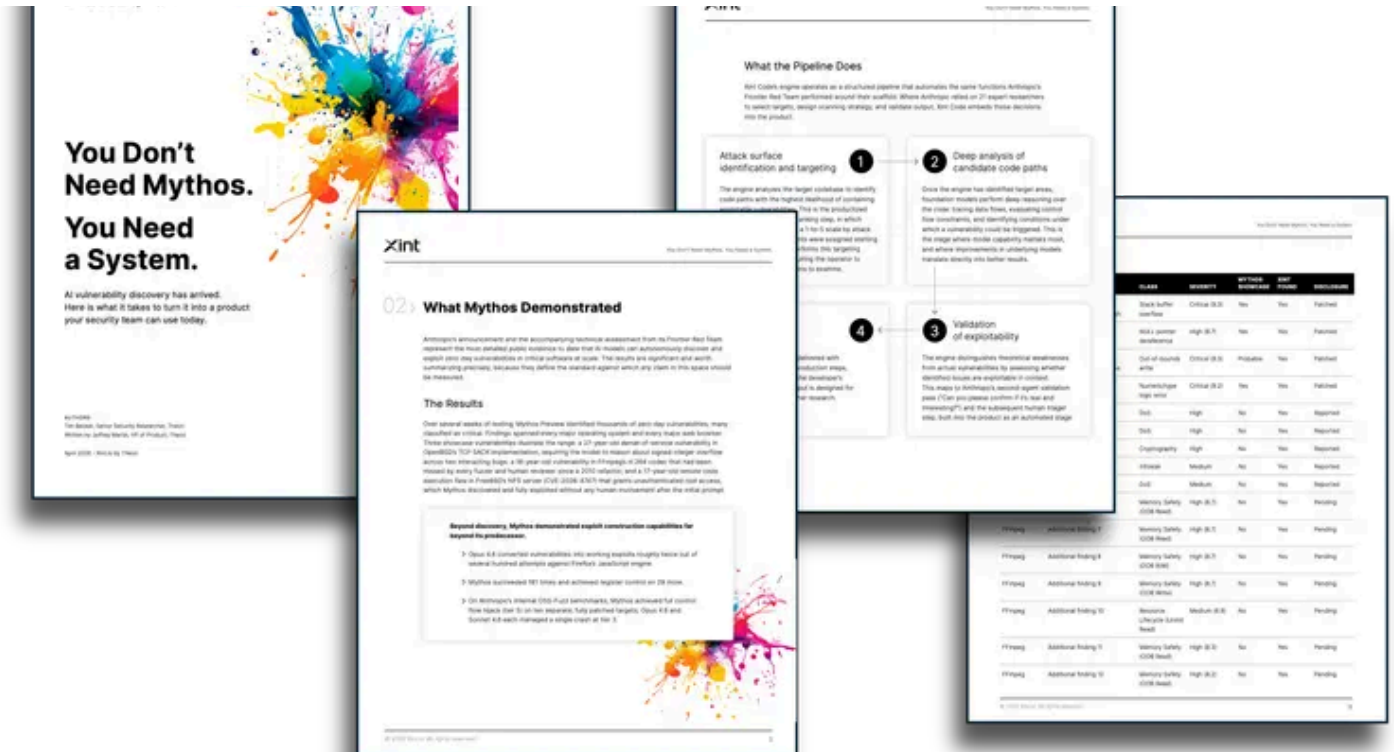
Theori BLOG

Empowering Innovation with Security

Explore expert insights into offensive security and threat intelligence.

See All AI for Security Security for AI Vulnerability Research Web2 Security

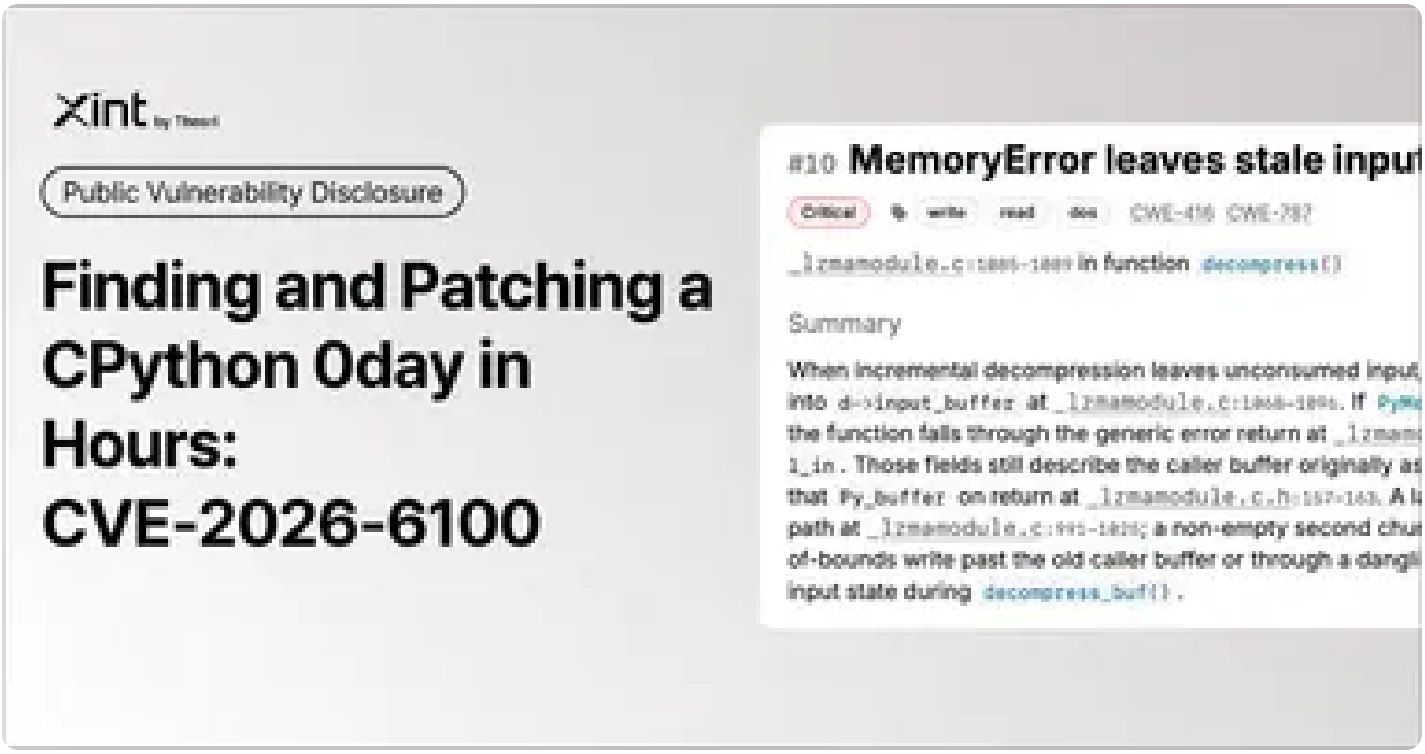
AIxCC



The Frontier Isn't the Model: Why 'Good Enough' Reasoning + Scaffolding Is More Important

In this exclusive report, Xint researchers compare Mythos's publicly disclosed results versus what broadly available models can accomplish using advanced…

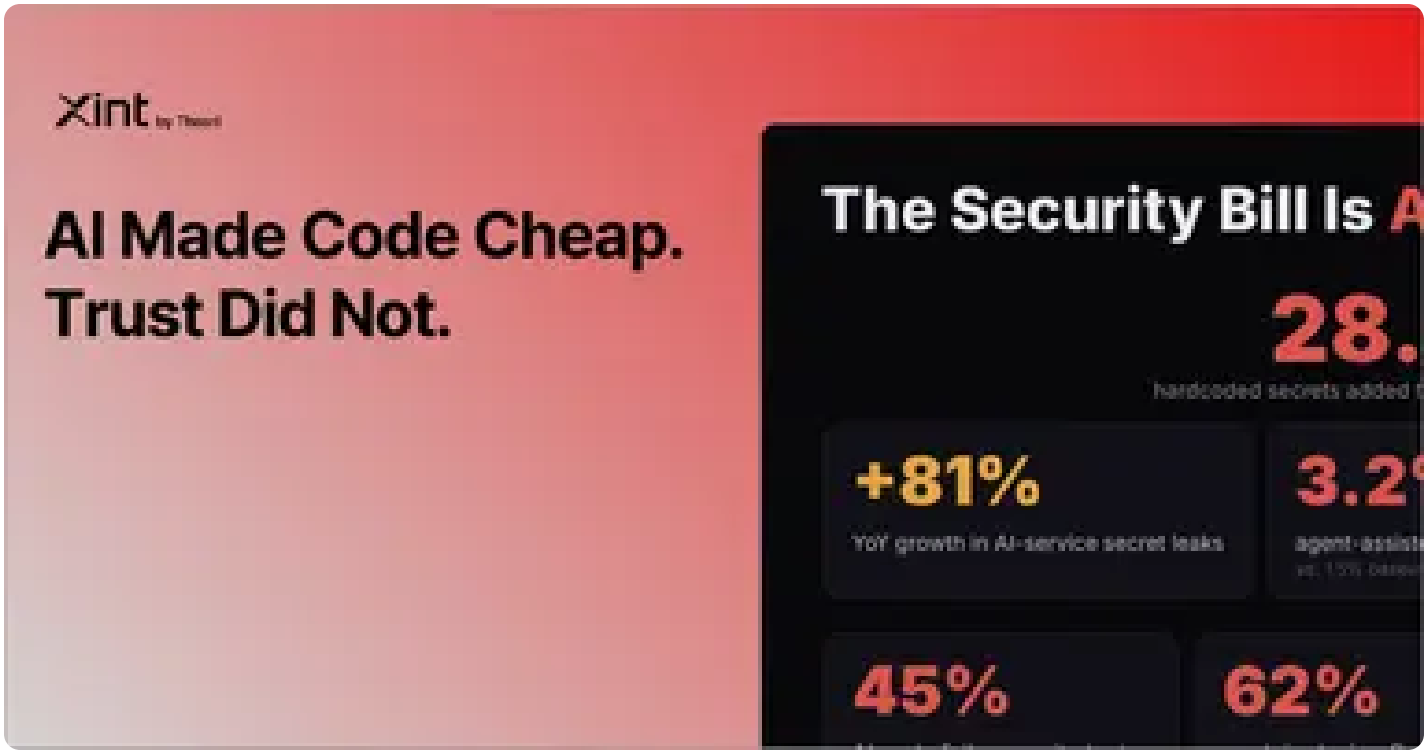
Apr 16, 2026 AI for Security



Finding and Patching a CPython 0day in Hours: CVE-2026-6100

A critical CPython CVE today took less than 45 minutes of human work to find, triage, and fix because of Xint Code

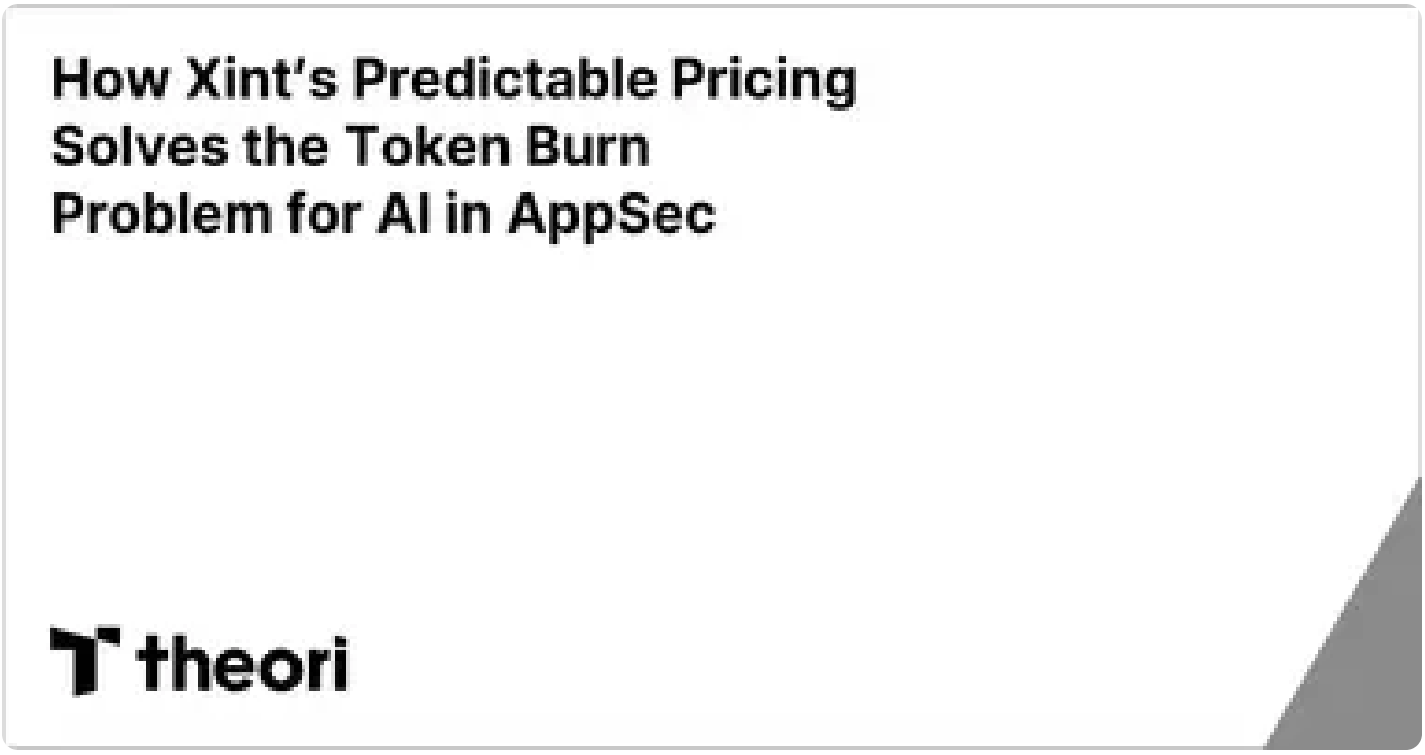
Apr 13, 2026 AI for Security



AI Made Code Cheap. Trust Did Not.

While code is abundant, assurance is scarce. The winners won't be the teams that generate the most code, it’ll be the teams that can prove it's safe.

Apr 13, 2026 AI for Security



How Xint’s Predictable Pricing Solves the Token Burn Problem for AI in AppSec

Linear increases in code are leading to exponential token burn increases. Xint's orchestration brings clear, predictable pricing.

Apr 09, 2026 AI for Security



What are business logic vulnerabilities, and why are they so hard to catch?

Even secure-looking code can hide dangerous flaws. Learn why business logic vulnerabilities are hard to detect and why most scanners miss them.

Mar 06, 2026 AI for Security



Announcing Xint Code

Real Vulnerabilities. Actionable Results.

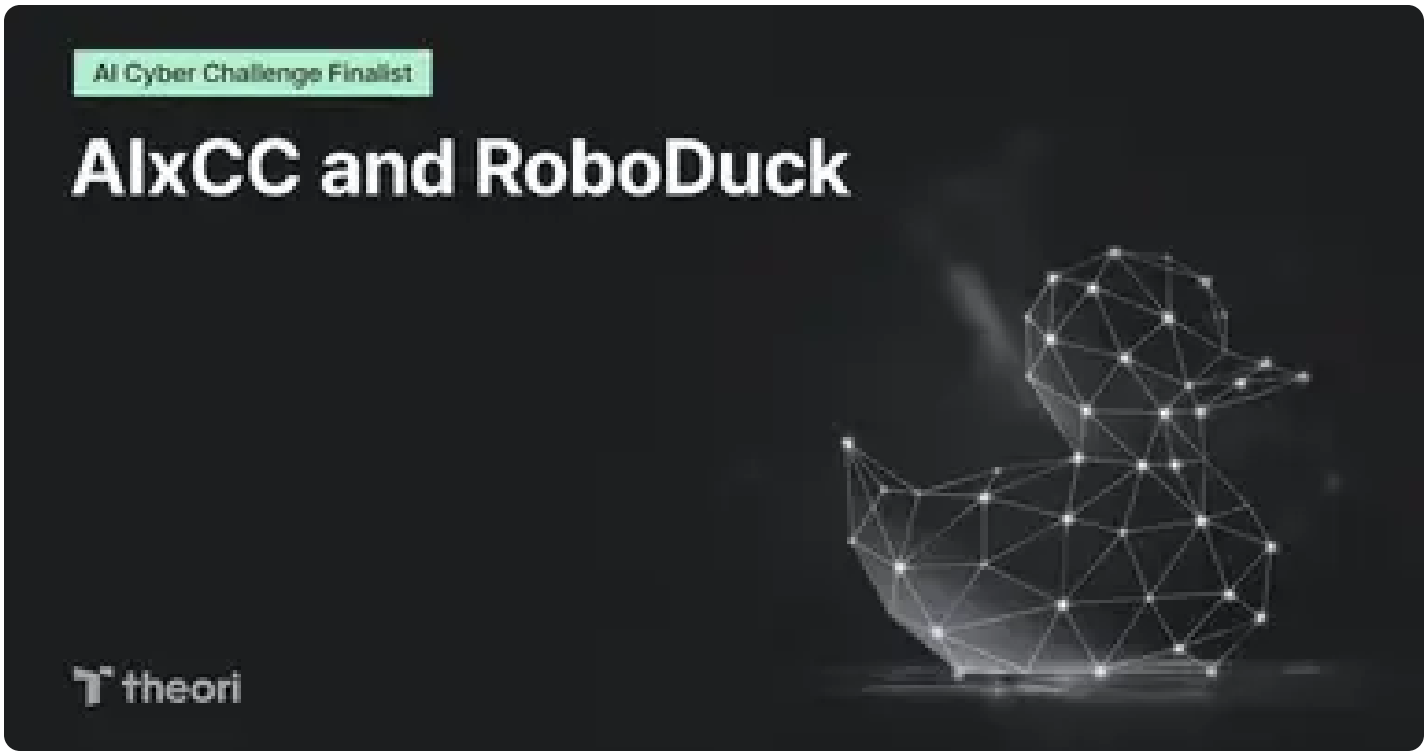
Xint Dec 15, 2025 AI for Security



Building Effective LLM Agents | AI Cyber Challenge

How we learned to build effective LLM agents for hacking at DARPA's AI Cyber Challenge (AIxCC)

Aug 08, 2025 AI for Security AIxCC



AI Cyber Challenge and Theori's RoboDuck

An introduction to DARPA's AI Cyber Challnge and Theori's third place cyber reasoning system

Aug 08, 2025 AI for Security AIxCC



Inside the brain of a hacking robot: Exploring traces | AI Cyber Challenge

Agent trajectory walkthroughs of a fully autonomous hacking system

Xint Aug 08, 2025 AI for Security AIxCC



How to Identify Phishing Scams

Learn how to spot phishing scams with expert tips recognizing suspicious emails, SMS, and fraudulent request for personal information.

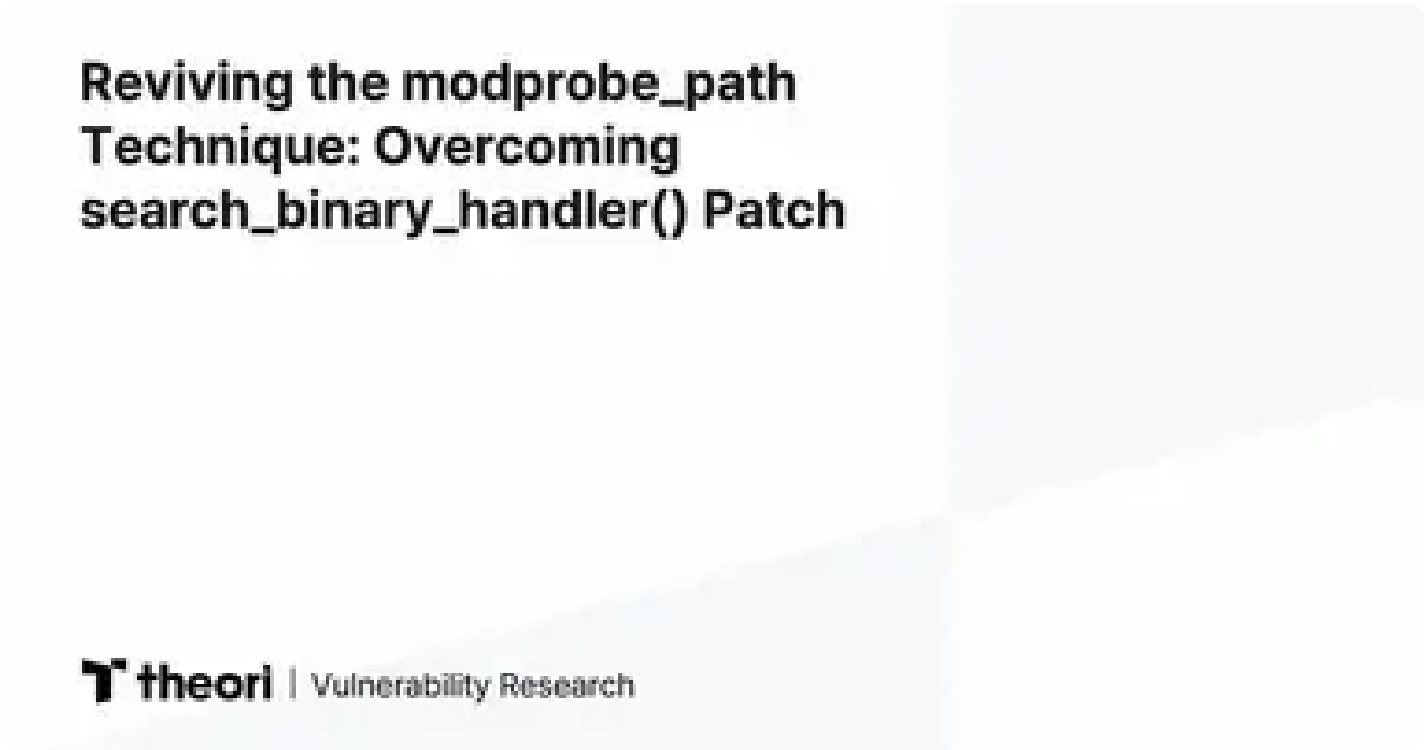
Apr 28, 2025 Vulnerability Research



Importance of Continuous Security: Lessons from the Bybit Case

In this article, we briefly look at the circumstances of the Bybit incident and discuss what countermeasures could have been implemented. Then, we discuss…

Xint Mar 27, 2025 AI for Security



Reviving the modprobe_path Technique: Overcoming search_binary_handler() Patch

A new approach to the Overwriting modprobe_path technique is introduced, addressing changes in the Upstream kernel that prevent triggering via dummy...

Mar 15, 2025 Vulnerability Research



Four Ways to Protect Your Legacy with Theori's Cybersecurity Solutions

Discover the top cybersecurity threats for 2025 and how Theori's innovative solutions can safeguard your business from evolving cyber risks and costly data…

Feb 16, 2025 Web2 Security



DeepSeek Security, Privacy, and Governance: Hidden Risks in Open-Source AI

This post examines DeepSeek's security gaps, privacy practices, and open-source AI risks, offering practical advice for users and developers.

Feb 06, 2025 Security for AI



The True Cost of Siloed Security Tools

Security silos occur when different security tools, teams, or systems operate in isolation, unable to effectively share data or communicate.

Dec 20, 2024 AI for Security



Finding Vulnerabilities in Firmware with Static Analysis Platform QueryX

QueryX, Theori’s program analysis platform, automates variant analysis for vulnerability detection. Learn how its taint analysis module uncovered CVE-202…

Nov 06, 2024 Vulnerability Research



Side Effects: When Continuous Development Introduces Security Threats

Dive into five significant security risks that emerged as unintended consequences of new feature development.

Nov 04, 2024 Web2 Security



Top 5 Features Your ASM Solution Must Have

So you know what ASM is and why you need it—but which features are crucial? Here’s the run down.

Oct 24, 2024 AI for Security



Offensive Security with Large Language Models (2)

How LLMs are changing the game for static analysis—especially when source code is available.

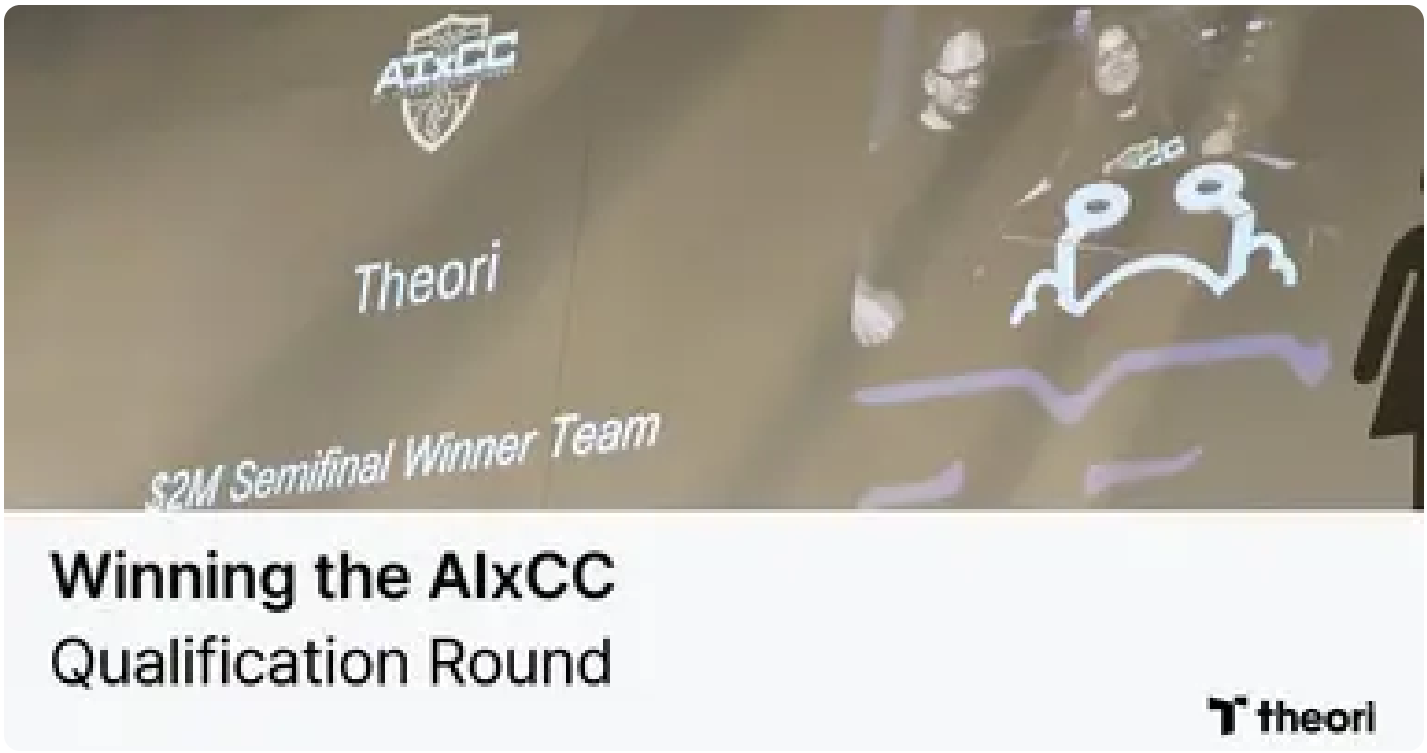
Sep 30, 2024 AI for Security



Offensive Security with Large Language Models (1)

Applications of larage language models in offensive security

Xint Sep 27, 2024 AI for Security



Winning the AIxCC Qualification Round

Theori’s Cyber Reasoning System (CRS) “Robo Duck” not only cleared the bar to get us $2M and a spot at the AIxCC finals in 2025, it also got the first place…

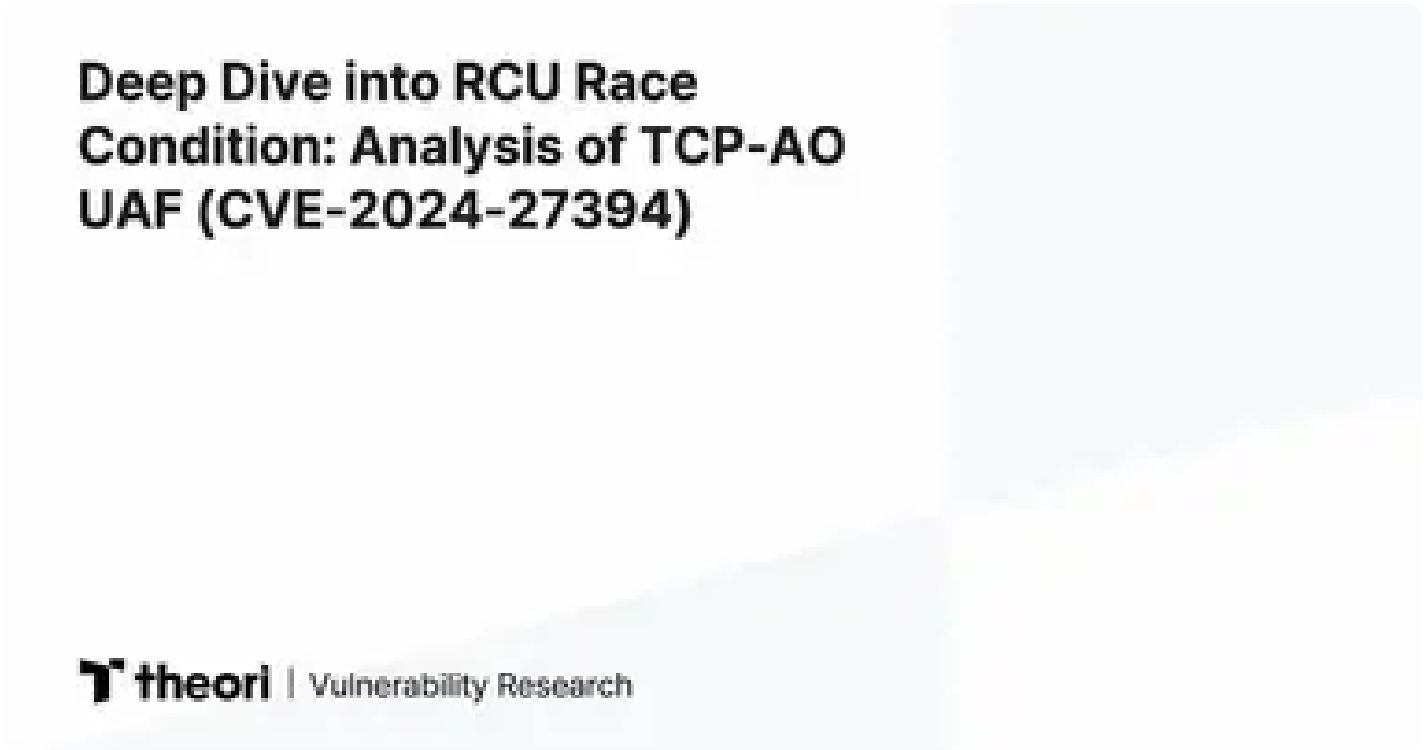
Sep 23, 2024 AI for Security



Top Penetration Testing Solutions for IT Security: 2024 Guide

The top 7penetration testing tools of 2024 for hackers and for businesses.

Sep 11, 2024 AI for Security



Deep Dive into RCU Race Condition: Analysis of TCP-AO UAF (CVE-2024–27394)

CVE-2024-27394 is a TCP-AO Use-After-Free vulnerability caused by improper RCU API usage. Read the in-depth analysis and reliable triggering technique.

Sep 03, 2024 Vulnerability Research



Offensive Security vs. Defensive Security: Navigating the Two Pillars of Cybersecurity

Explore how offensive and defensive security strategies work together to protect against cyber threats.

Aug 30, 2024 Web2 Security



A Deep Dive into the CoSoSys EndPoint Protector Exploit: Remote Code Execution

Four critical RCE vulnerabilities (CVE-2024-36072 to CVE-2024-36075) in CoSoSys Endpoint Protector were identified, allowing full server and client compromise....

Aug 29, 2024 Web2 Security



Chaining N-days to Compromise All: Part 6 — Windows Kernel LPE: Get SYSTEM

The final part of the N-day exploit series analyzes CVE-2023-36802, a privilege escalation vulnerability in mskssrv.sys, used to gain SYSTEM access on a VMwar...

May 21, 2024 Vulnerability Research



Chaining N-days to Compromise All: Part 5 — VMware Workstation Guest-to-Host Escape

CVE-2023-20869 was exploited to achieve arbitrary code execution on a VMware host from a guest system. Read the full technical analysis.

May 02, 2024 Vulnerability Research



Chaining N-days to Compromise All: Part 4 — VMware Workstation Information leakage

CVE-2023-34044, a variant of CVE-2023-20870, was exploited to extract critical information from a VMware host process. Read the in-depth analysis.

Apr 17, 2024 Vulnerability Research



Chaining N-days to Compromise All: Part 3 — Windows Driver LPE: Medium to System

CVE-2023-29360, a logic bug in the mskssrv.sys driver, was exploited to escalate privileges to SYSTEM in a 1-day full chain attack. Read the detailed breakdown.

Apr 08, 2024 Vulnerability Research



Chaining N-days to Compromise All: Part 2 — Windows Kernel LPE (a.k.a Chrome Sandbox Escape)

CVE-2023-21674, a Windows kernel UAF vulnerability, was used to escape the Chrome sandbox in a 1-day full chain exploit. Read the detailed analysis.

Mar 31, 2024 Vulnerability Research



Chaining N-days to Compromise All: Part 1 — Chrome Renderer RCE

This post begins our series on the 1-day exploit chain demoed on X, focusing on a Chrome renderer exploit, CVE-2023-3079, a type confusion bug in V8.

Mar 17, 2024 Vulnerability Research

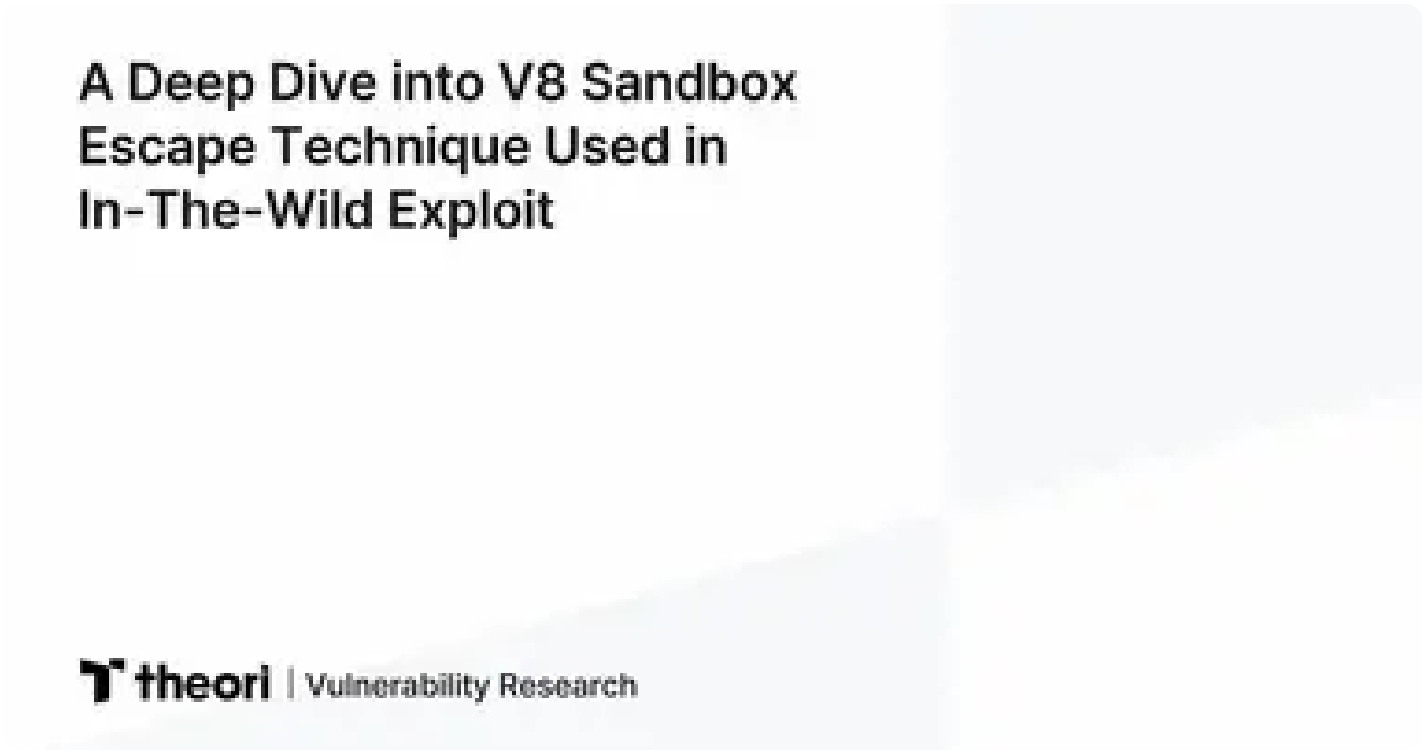


Fermium-252 : The Cyber Threat Intelligence Database

Fermium-252 is a premier vulnerability intelligence platform providing real-time tracking of 1-day exploits, PoCs, and in-depth reports. Stay ahead of cyber threa...

Mar 03, 2024 Vulnerability Research

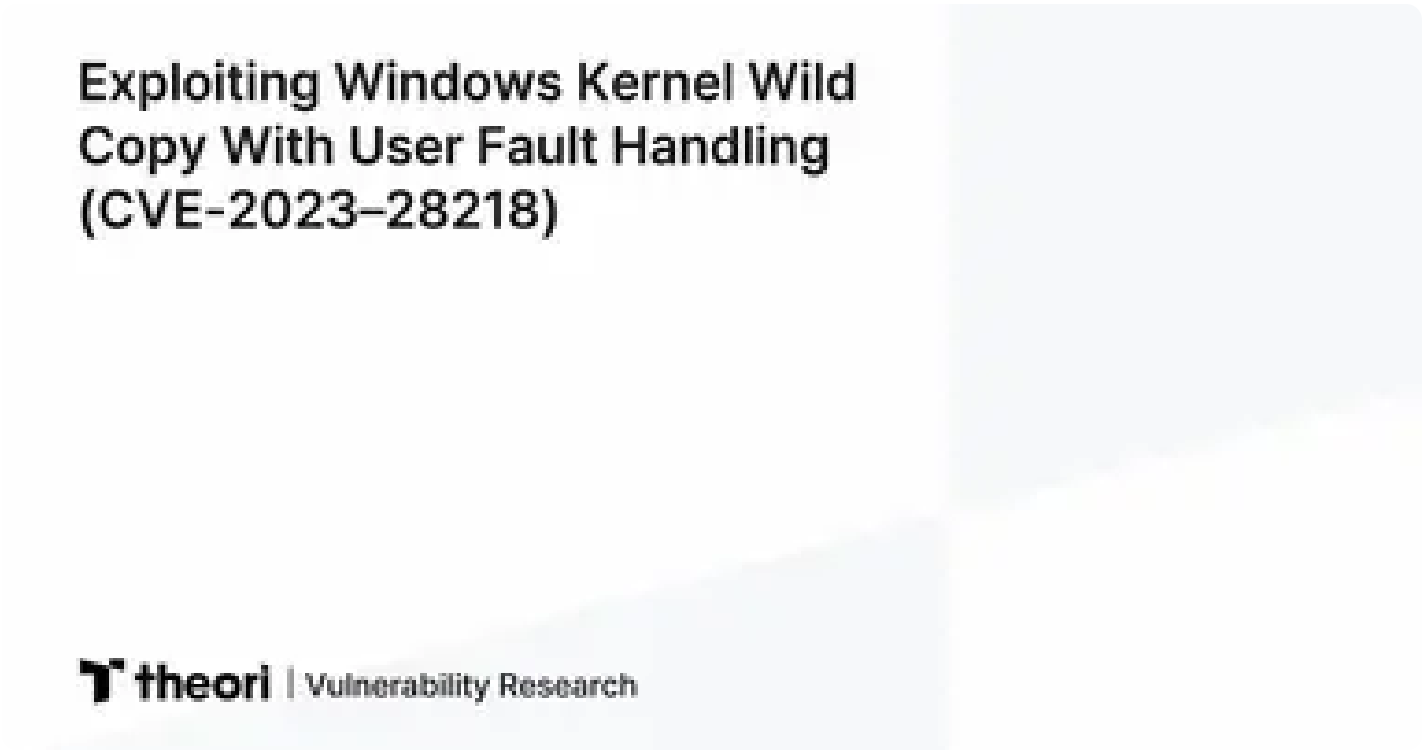
Theori © 2026 All rights reserved.



A Deep Dive into V8 Sandbox Escape Technique Used in In-The-Wild Exploit

We bypassed the V8 sandbox using a raw pointer in WasmIndirectFunctionTable, enabling arbitrary write and code execution. Read our deep dive into the exploit.

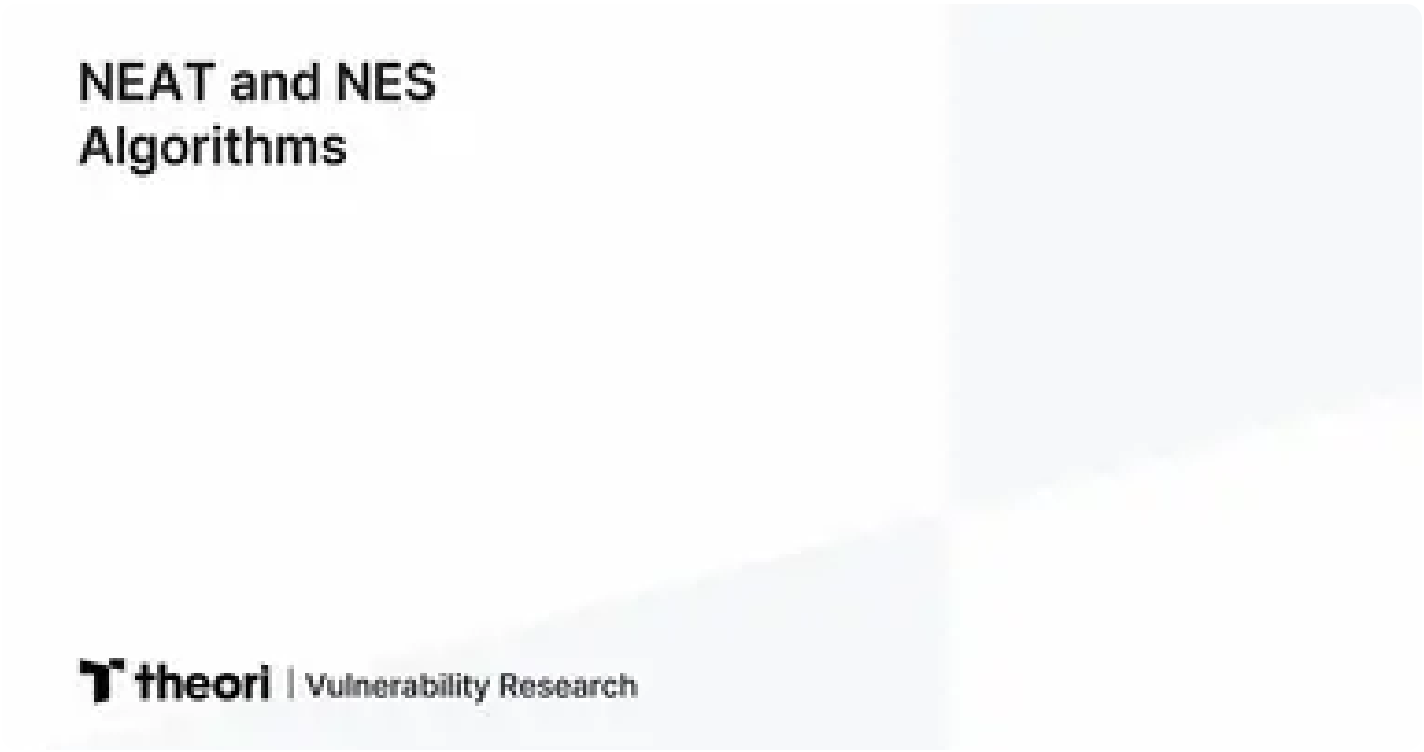
Jan 25, 2024 Vulnerability Research



Exploiting Windows Kernel Wild Copy With User Fault Handling (CVE-2023–28218)

At Hexacon 2023, we presented our Windows kernel security research, uncovering CVE-2023-28218, a heap overflow in afd.sys. Read our exploit analysis and…

Nov 09, 2023 Vulnerability Research



NEAT and NES Algorithms

We reverse-engineered NEAT and NES, two unpublished symmetric encryption algorithms from South Korea’s GPKI cryptography library. Read our analysis and…

Apr 20, 2023 Vulnerability Research



Linux Kernel Exploit (CVE-2022–32250) with mqueue

We exploited CVE-2022-32250, a use-after-free vulnerability in Linux Netfilter, to achieve root on Ubuntu 22.04. Learn how we bypassed KASLR and modified…

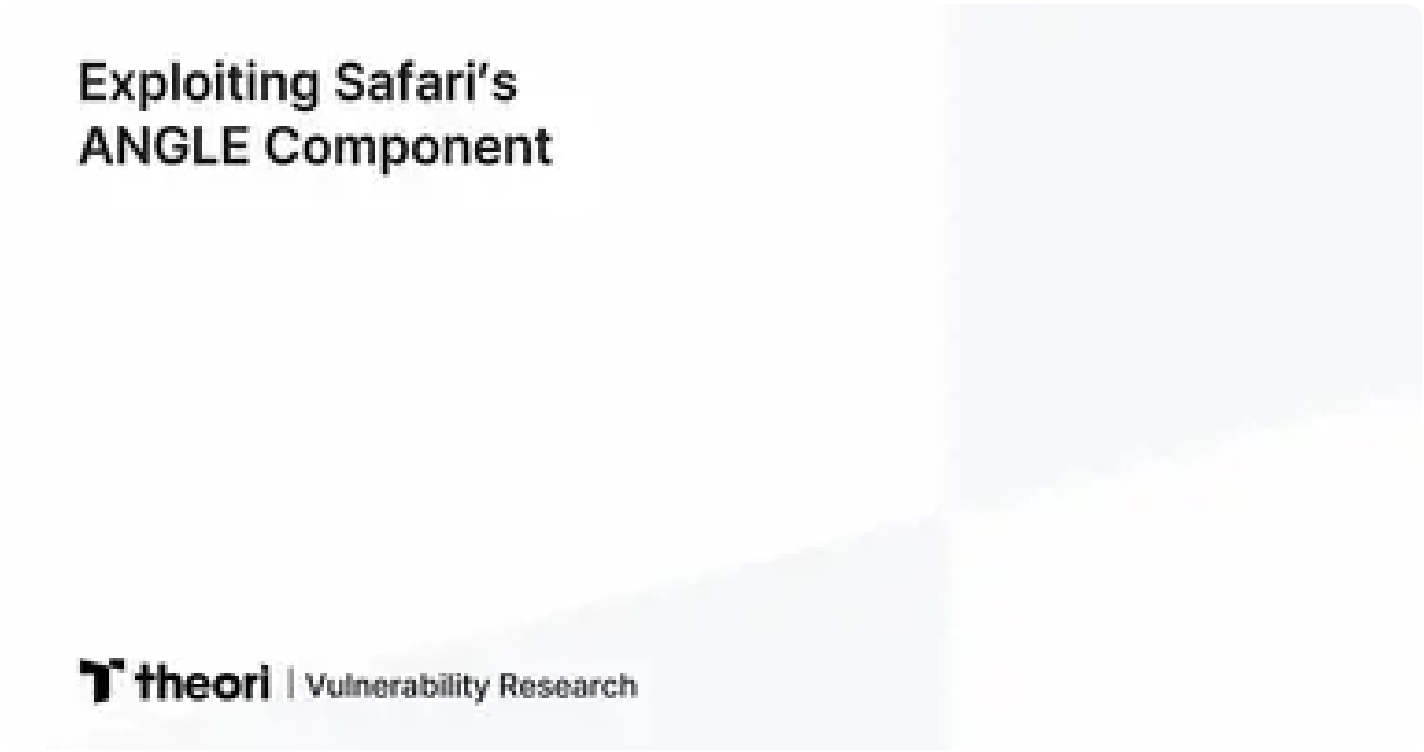
Aug 23, 2022 Vulnerability Research



Binary-searching into CVMServer

While analyzing the patch for CVE-2021-30724, we discovered a new uninitialized memory vulnerability (CVE-2022-26721) in macOS's CVMServer. Read our...

Jun 16, 2022 Vulnerability Research



Exploiting Safari’s ANGLE Component

We discovered CVE-2022-26717, an exploitable bug in WebKit's WebGL component affecting Safari on macOS and iOS. Read our analysis and exploitati…

May 17, 2022 Vulnerability Research



Patch Gapping a Safari Type Confusion

Safari 14.1 introduced AudioWorklets, but a newly patched type confusion bug left iOS versions vulnerable for weeks. We share our root cause analysis and exploit...

May 24, 2021 Vulnerability Research



Compromising virtualization without attacking the hypervisor

Discover CVE-2020-27675 (XSA-331), a denial-of-service and potential out-of-bounds write vulnerability in the Xen paravirtualization driver, and learn how it...

Oct 20, 2020 Vulnerability Research



Cleanly Escaping the Chrome Sandbox

Learn how we discovered and exploited Issue 1062091, a use-after-free (UAF) vulnerability in Chrome and Chromium-based Edge, leading to a sandbox escape.

Apr 19, 2020 Vulnerability Research



Receiving NRSC-5

We have implemented an NRSC-5-C digital radio receiver and released it as open source on GitHub. Explore IBOC-based hybrid broadcasting and security researc...

Jun 08, 2017 Vulnerability Research



Chakra JIT CFG Bypass

Learn how attackers bypassed Microsoft's Control Flow Guard (CFG) in Internet Explorer and Edge. We break down our PoC exploit, mitigation bypass, and the…

Dec 13, 2016 Vulnerability Research



Patch Analysis of MS16–063 (jscript9.dll)

Microsoft's MS16-063 patch fixed a critical memory corruption vulnerability in jscript9.dll (TypedArray & DataView) affecting Internet Explorer. Read our analys...

Jun 26, 2016 Vulnerability Research



Patch Analysis of CVE-2016–0189

Microsoft's MS16-051 patch addressed a critical Internet Explorer vulnerability (CVE-2016-0189) exploited in South Korea. Explore our in-depth analysis, patch…

Jun 21, 2016 Vulnerability Research