V8 Sandbox escape/bypass/violation and VR collection

A collection of links related to V8 sandbox VR and exploitation

Contents

IssueTracker

2023: "issue id: 40940619, V8 Sandbox escape due to type tags in ExternalPointerTable being too coarse for Embedder Objects"

2023: "issue id: 40940623, V8 Sandbox escape due to coarse type-checking for Foreigns"

2024: "issue id: 42204606, Mitigate sandbox escapes in RegExp"

2024: "issue id: 336507783, V8 Sandbox: Prevent Wasm-based sandbox escapes "

2024: "issue id: 327732554, V8 sandbox violation due to signed comparison of (untrusted) string length against buffer size"

2024: "issue id: 326086002, Sandbox violations due to (exhaustive) switches over enums when the code after the switch has UB"

2024: "issue id: 327732554, V8 sandbox violation in v8::internal::Builtins::code"

2024: "issue id: 328692018, V8 sandbox violation in v8::bigint::Digits::read_4byte_aligned"

PROF

2024: "issue id: 328858270, V8 sandbox violation in v8::internal::GetBailoutReason"

2024: "issue id: 332475841, V8 sandbox violation in v8::internal::ElementsKindToString"

2024: "issue id: 41487854, V8 sandbox violation in Builtins_StarWideHandler"

2024: "issue id: 323736727, V8 sandbox violation in Builtins_DeoptimizationEntry_Eager"

2024: "issue id: 323694399, V8 sandbox violation in Builtins_DeoptimizationEntry_Eager"

2024: "issue id: 323696394, V8 sandbox violation in Builtins_DeoptimizationEntry_Eager"

2024: "issue id: 323690010, V8 sandbox violation in Builtins_DeoptimizationEntry_Eager"

2024: "issue id: 327550517, V8 sandbox violation in v8::internal::ArrayBufferSweeper::Detach"

2024: "issue id: 324343442, V8 sandbox violation in v8::internal::SemiSpace::FixPagesFlags"

2024: "issue id: 324482838, V8 sandbox violation in v8::internal::maglev::MaglevGraphBuilder::BuildAllocateFastObject"

2024: "issue id: 326109866, Use-after-poison in v8::internal::compiler::MapData::instance_type"

2024: "issue id: 327719160, V8 sandbox violation in v8::internal::MarkCompactCollector::ProcessMarkingWorklist"

2024: "issue id: 327827222, V8 sandbox violation in v8::internal::ConcurrentMarking::RunMajor"

2024: "issue id: 329425726, V8 sandbox violation in v8::internal::Scavenger::IterateAndScavengePromotedObject"

2024: "issue id: 329886545, V8 sandbox violation in v8::internal::JSFunction::CalculateExpectedNofProperties"

2024: "issue id: 330219140, V8 sandbox violation in unsigned int v8::base::AsAtomicImpl::Relaxed_Load"

2024: "issue id: 330385840, V8 sandbox violation in v8::internal::Code::kind"

2024: "issue id: 330404819, V8 Sandbox escape via regexp"

2024: "issue id: 329781445, V8 sandbox violation in v8::internal::Scavenger::IterateAndScavengePromotedObject"

2024: "issue id: 330563095, WebCodecs VideoFrame Race Condition UAF Write to RCE" by Seunghyun Lee(@0x10n) [Pwn2Own 2024]

2024: "issue id: 331042197, V8 sandbox violation in v8::internal::Scavenger::IterateAndScavengePromotedObject"

2024: "issue id: 330922416, V8 sandbox violation in v8::internal::ArrayBufferExtension::backing_store"

2024: "issue id: 331036491, V8 sandbox violation in icu_73::Locale::getBaseName"

PROF

2024: "issue id: 330096629, V8 sandbox violation in icu_73::RelativeDateTimeFormatter::getFormatStyle"

2024: "issue id: 331241020, V8 sandbox violation and memory corruption due to buffer overflow in compiler"

2024: "issue id: 331883947, V8 sandbox violation in v8::internal::Managed<icu_73::Locale>::GetSharedPtrPtr"

2024: "issue id: 331837303, V8 sandbox violation in v8::internal::maglev::MaglevGraphBuilder::TryBuildInlinedAllocatedContext"

2024: "issue id: 331042216, V8 sandbox violation in v8::internal::LazyCreateDateIntervalFormat"

2024: "issue id: 333065495, V8 sandbox violation in v8::internal::MemoryChunkMetadata::heap"

2024: "issue id: 329920544, V8 sandbox violation in v8::internal::Managed<icu_73::number::LocalizedNumberFormatter>::GetSharedPtrPtr"

2024: "issue id: 330800450, V8 sandbox violation in unsigned long v8::base::AsAtomicImpl::Relaxed_Load"

2024: "issue id: 335763881, V8 sandbox violation in v8::internal::TranslatedState::CreateNextTranslatedValue"

2024: "issue id: 335544065, V8 sandbox violation in Builtins_DeoptimizationEntry_Eager"

2024: "issue id: 335322609, V8 sandbox violation in v8::internal::maglev::CapturedObject::set"

2024: "issue id: 335810507, V8 sandbox violation in v8::internal::ToLatin1Lower"

2024: "issue id: 337094992, V8 sandbox violation in v8::internal::ArrayBufferExtension::backing_store"

2024: "issue id: 336655186, V8 sandbox violation in v8::internal::Scavenger::IterateAndScavengePromotedObject"

2024: "issue id: 333829668, V8 sandbox violation in v8::base::Flags<v8::internal::MemoryChunk::Flag, unsigned long, unsigned long>::"

2024: "issue id: 327473161, V8 sandbox violation in v8::internal::TranslatedState::CreateNextTranslatedValue"

2024: "issue id: 334120897, V8 Sandbox Bypass: wasm function signature confusion leading to out of sandbox arbitrary read/write "

2024: "issue id: 336648007, V8 sandbox violation in v8::internal::maglev::CapturedObject::set"

2024: "issue id: 343407073, V8 Sandbox Bypass: control-flow hijacking via WASM Table Indirect call" [Edouard Bochin (@le_douds) and Tao Yan (@Ga1ois)]

2024: "issue id: 339141292, V8 sandbox violation in Builtins_JSToJSWrapper"

2024: "issue id: 339310133, V8 sandbox violation in v8::internal::maglev::CapturedObject::set"

PROF

2024: "issue id: 339517309, V8 sandbox violation in v8::internal::maglev::CapturedObject::set"

2024: "issue id: 338342089, V8 sandbox violation in v8::internal::wasm::name"

2024: "Generate heap sandbox tags for IDL-based types"

2024: "issue id: 337941142, V8 sandbox violation in v8::base::Flags<v8::internal::MemoryChunk::Flag, unsigned long, unsigned long>::"

2024: "issue id: 342451736, V8 sandbox violation in void v8::internal::BodyDescriptorBase::IterateTrustedPointer<v8::internal::MainM "

2024: "issue id: 342866373, V8 Sandbox Bypass: JSToWasmWrapperAsm accessible and allows type confusion"

2024: "issue id: 338342091, V8 sandbox violation in Builtins_JSToJSWrapper"

2024: "issue id: 337547182, V8 sandbox violation in Builtins_SuspendGeneratorHandler"

2024: "issue id: 342297062, V8 sandbox violation if SFI::formal_parameter_count doesn't match the parameter count of a function's code"

2024: "issue id: 343801366, V8 Sandbox Bypass: Incomplete hardening of the experimental regex engine"

2024: "issue id: 344943044, V8 sandbox violation in v8::internal::maglev::MaglevGraphBuilder::GetValueNodeFromCapturedValue"

2024: "issue id: 344963941, V8 Sandbox Bypass: Irregexp engine bytecode modification leads to arbitrary read/write outside the sandbox"

2024: "issue id: 346799730, Regexp backtrack stack can underflow"

2024: "issue id: 339043698, V8 sandbox violation in unsigned char v8::base::ReadUnalignedValue"

2024: "issue id: 348324480, OutsideSandboxOrInReadonlySpace checks in-sandbox data"

2024: "issue id: 349517592, Wasm FeedbackMaker OOB accesses"

2024: "issue id: 345547973, V8 sandbox violation in v8::internal::wasm::name"

2024: "issue id: 349563054, V8 Sandbox Bypass: UAF by manipulating Managed"

2024: "issue id: 349641090, V8 sandbox violation in v8::internal::compiler::MapData::instance_type"

2024: "issue id: 337906704, V8 sandbox violation in v8::internal::OldLargeObjectSpace::PromoteNewLargeObject"

2024: "issue id: 348793147, V8 Sandbox Bypass: AAR/W via table import signature check bypass"

2024: "issue id: 351327767, WebAssembly OOB memory access due to cached memory index confusion"

2024: "issue id: 352446085, V8 Sandbox Bypass: AAR/W via WASM import race condition leading to broken runtime bounds check with memory64"

PROF

2024: "issue id: 349502157, V8 Sandbox Bypass: AAR/W via table set OOB SBXCHECK_LT() bypass"

2024: "issue id: 349529650, V8 Sandbox Bypass: AAR/W via function import signature check race"

2024: "issue id: 352689356, V8 Sandbox Bypass: AAR/W via WASM function signature confusion in TurboFan call_ref"

Articles

2022: "Code Execution in Chromium’s V8 Heap Sandbox"

2022: "KITCTFCTF 2022 V8 Heap Sandbox Escape"

2022: "memory hole"[DiceCTF 2022]

2022: "Memory Hole: Breaking V8 Heap Sandbox"[DiceCTF 2022]

2023: "Use Native Pointer of Function to Bypass The Latest Chrome v8 Sandbox (exp of issue1378239)"

2023: "Use Wasm to Bypass Latest Chrome v8sbx Again"

2023: "Exploiting Zenbleed from Chrome"

2023: "Exploring Historical V8 Heap Sandbox Escapes I"

2023: "Abusing Liftoff assembly and efficiently escaping from sbx(@r3tr074)"

2023: "Start Your Engines - Capturing the First Flag in Google's New v8CTF"

2024: "Google Chrome V8 CVE-2024-0517 Out-of-Bounds Write Code Execution"

2024: "The V8 Sandbox"

2024: "Issue-1472121 : Exploit out-of-bound CloneObjectIC type confusion"

2024: "From object transition to RCE in the Chrome renderer"

2024: "Attack of the clones: Getting RCE in Chrome’s renderer with duplicate object properties"

2024: "A Deep Dive into V8 Sandbox Escape Technique Used in In-The-Wild Exploit"

2024: "CVE-2024-2887: A Pwn2Own Winning Bug in Google Chrome"

2024: "Breaking V8 Sandbox with Trusted Pointer Table"[HITCON CTF 2024]

2024: "HITCON CTF QUAL 2024 Pwn Challenge Part 1 - Halloween and v8sbx"[HITCON CTF 2024]

2024: "SSD Advisory – Google Chrome RCE(Seunghyun Lee (@0x10n)"[TyphoonPWN 2024]

Papers & Slides

2022: "Sandboxing V8(Samuel Groß, @5aelo)"

2023: "Modern chrome exploit chain development"[POC2023 - @numencyber]

PROF

2024: "The V8 Heap Sandbox(Samuel Groß, @5aelo)"[OffensiveCon 2024]

2024: "A Chrome/Edge RCE via V8 WASM Type Confusion by Manfred Paul(@_manfp)"[Pwn2Own Vancouver 2024]

2024: "Google Chrome Renderer Only RCE by Seunghyun Lee (@0x10n)"[Pwn2Own Vancouver 2024]

2024: "Evolution of the protections of the V8 JSE"[slides][Full Article][SSTIC2024]

2024: "From the Vulnerability to the Victory: A Chrome Renderer 1-Day Exploit’s Journey to v8CTF Glory"[TyphoonCon 2024]

2024: "TIKTAG: Breaking ARM’s Memory Tagging Extension with Speculative Execution"

2024: "Let the Cache Cache and Let the WebAssembly Assemble: Knockin' on Chrome's Shell"[blackhat USA 2024]

2024: "V8 Sandbox Escape Write Up - Edouard Bochin (@le_douds) and Tao Yan (@Ga1ois)"[Pwn2Own Vancouver 2024]

2024: "Bypassing the V8 sandbox protection mechanism"[OFFZONE 2024]

2024: "Chrome Exploitation: from Zero to Heap-Sandbox Escape"[BSides Oslo 2024][matteo malvica]

Design documents

2019: "Compressed pointers in V8"

2021: "V8 Sandbox"

2022: "V8 Sandbox - Address Space"

2022: "V8 Sandbox - Sandboxed Pointers"

2022: "V8 Sandbox - External Pointer Sandboxing"

2022: "V8 Sandbox - Code Pointer Sandboxing"

2023: "V8 Sandbox - Glossary"

2023: "V8 Sandbox - Trusted Space"

2024: "Multiple sandboxes aka sandbox per isolate group"

2024: "V8 Sandbox - Hardware Support"

2024: "V8 Sandbox - Embedder Pointer Sandboxing"

2024: "V8 Sandbox + Leaptiering"