TYPE

Longer presentation

TITLE

GHunter: Universal Prototype Pollution Gadgets in JavaScript Runtimes

AUTHORS

Eric Cornelissen, KTH Royal Institute of Technology *(**Presenting**)*
Mikhail Shcherbakov, KTH Royal Institute of Technology
Musard Balliu, KTH Royal Institute of Technology

ABSTRACT

Prototype pollution is a vulnerability that affects JavaScript code, leading to high impact attacks such as arbitrary code execution and privilege escalation. The vulnerability is rooted in JavaScript's prototype-based inheritance, enabling attackers to inject arbitrary properties into an object's prototype at runtime. The impact of prototype pollution depends on the existence of otherwise benign pieces of code, so-called gadgets, which inadvertently read from these attacker-controlled properties to execute security-sensitive operations. While prior work in this area has been focussed on gadgets in third-party libraries and client-side applications, this work instead focuses on gadgets in JavaScript runtimes motivated by their universality.

This presentation will present *GHunter*, the first pipeline to systematically detect gadgets in V8-based JavaScript runtimes, in particular Node.js and Deno. *GHunter* supports a lightweight dynamic taint analysis to automatically identify candidate gadgets which we validate manually to derive proof-of-concept exploits. We implement *GHunter* by modifying the V8 engine and the targeted runtimes along with features for facilitating manual validation. Driven by the comprehensive test suites of Node.js and Deno, we use *GHunter* in a systematic study of gadgets in these runtimes. We identified a total of 55 new gadgets in Node.js and 57 gadgets in Deno, including but not limited to vulnerabilities such as arbitrary code execution (16), privilege escalation (23), and path traversal (13).