DOYENSEC

Security Advisory

Regular Expression Denial of service (ReDoS) in npm/ssri

Created by Ben Caller
10th Feb 2021

Overview

This document provides technical details of a Regular Expression Denial of Service vulnerability in the ssri npm package from version 5.2.2 until the fix in version 8.0.1.

About Us

Doyensec is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Research is one of our founding principles and we invest heavily in it. By discovering new vulnerabilities and attack techniques, we constantly improve our capabilities and contribute to secure the applications we all use.

Copyright 2021. Doyensec LLC. All rights reserved.

Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except by reformatting it, and that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar, provided that due credit is given. The information in the advisory is believed to be accurate at the time of publishing based on currently available information, and it is provided as-is, as a free service to the community by Doyensec LLC. There are no warranties with regard to this information, and Doyensec LLC does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Regular Expression Denial of service (ReDoS) in npm/ssri	
Vendor	https://npmjs.com
Severity	Low
Vulnerability Class	Denial of Service
Component	ssri
Status	Fixed
CVE	CVE-2021-27290
Credits	Ben Caller of Doyensec

Summary

The npm package ssri processes SRIs using a regular expression which is vulnerable to Regular Expression Denial of Service (REDoS). Malicious SRIs could take an extremely long time to process, leading to Denial of Service. This issue only affects consumers using the `strict` option.

Technical Description

The vulnerable regular expression is:

```
const STRICT_SRI_REGEX = /^([^-]+)-([A-Za-z0-9+/=]{44,88})(\?[\x21-\x7E]*)*$/
```

https://github.com/npm/ssri/blob/41b764f91eda13867745f8d97c624c316e9c162e/index.js#L12

An attempt had been made to correct quadratic complexity worst-case behavior (assigned CVE-2018-7651) in commit https://github.com/npm/ssri/commit/d0ebcdc. However, the commit actually made the REDoS situation significantly worse, as the regex now backtracks with exponential worst-case complexity.

The section at the end `(\?[\x21-\x7E]*)*$` can be abused by sending a long string of question marks (`\x3f`) followed by a character not in `[\x21-\x7e]`.

The complexity is exponential: each extra question mark doubles the processing time.

If the `strict` option is set to false (the default), a non-vulnerable regular expression is used instead.

Proof-of-Concept

Run the following NodeJS code:

```
require('ssri').parse('sha512-00000000000000000000000000000000000000000000000000' +
'?'.repeat(35) + '\x1f', {strict: true})
```

Remediation

The maintainers have released an update (8.0.1) to address this issue:

- https://github.com/npm/ssri/releases/tag/v8.0.1
- Commit https://github.com/npm/ssri/commit/76e223317d971

Disclosure Timeline

2020-12-07	Vulnerability disclosed via email to security@npmjs
2020-12-18	Reply stating to contact maintainers from `npm owner ls ssri`
2020-12-30	Vulnerability disclosed via email to the last active maintainer
2021-01-19	Vulnerability disclosed via email to three other maintainers
2021-01-19	Vulnerability patched
2021-01-27	Patch released as version 8.0.1
2021-03-11	Doyensec advisory published