Command Injection Vulnerability In The Google-It NPM Package

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT

Adar Zandberg Apr 26, 2021

Details Overview

Summary

Google-it is a Node.js package which allows its users to send search queries to Google and receive the results in a JSON format. When using the 'Open in browser' option in versions up to 1.6.2, google-it will unsafely concat the result's link retrieved from google to a shell command, potentially exposing the server to RCE.

Product

All versions of the google-it NPM package.

Impact

This issue may lead to remote code execution on a machine running the google-it.

Steps To Reproduce

Exploitation is possible through several different vectors, using specially constructed text which will then be concatenated to an OS command and run on the system:
A man in the middle intercepting the reply from google may replace the href element of a result with a malicious command. For example:

```
; touch HACKED;
```

An actual result indexed by Google may contain a malicious url with an included OS command separated by special shell metacharacters. For example:

```
https://www.website.com/?a=`touch${IFS}HACKED`
```

If a user uses a query that will include this result, a `touch HACKED` command will be executed on the local system.

Expected Result:

A file named `HACKED` has been created.

Remediation

No fix is currently available. The only solution for now is to set the `config.open` to `false` when using google-it.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. Vulnerable code lib/googleIt.js#L57
2. Vulnerable code src/googleIt.js#L33