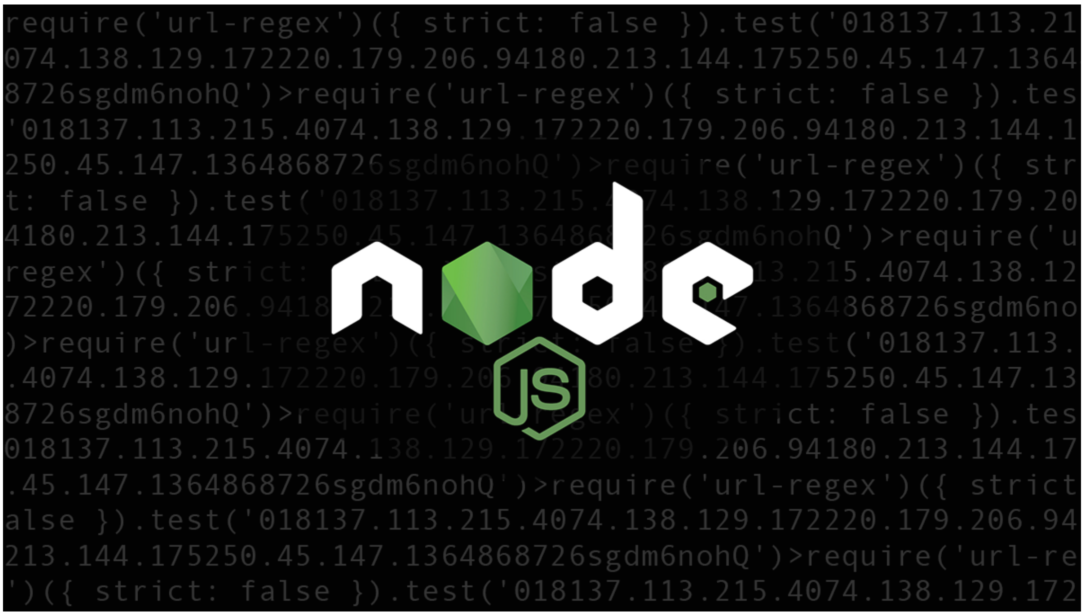
The Daily Swig
Cybersecurity news and views

# Node.js developers fix high-risk vulnerability that could allow remote domain hijacking

Jessica Haworth 12 August 2021 at 13:09 UTC

Vulnerabilities Research RCE

*Users of the JS framework need to patch now*



A vulnerability in Node.js that could allow a remote actor to perform domain hijacking attacks has been fixed.

The maintainers of the JavaScript runtime environment have released a security advisory today (August 12) warning users to update to the latest version to protect against a series of bugs.

The first vulnerability (CVE-2021-3672/CVE-2021-2293) is an improper handling of untypical characters in domain names, which opened the door to remote code execution (RCE), or cross-site scripting (XSS) exploits.

The flaw, which was classed as high severity, also caused application crashes due to missing input validation of hostnames returned by Domain Name Servers in the Node.js DNS library.

This could lead to the output of wrong hostnames – causing domain hijacking – and injection vulnerabilities in applications using the library.

**Read more of the latest security vulnerability news**

A second vulnerability (CVE-2021-22939) is the incomplete validation of rejectUnauthorized parameter.

If the Node.js HTTPS API was used incorrectly and undefined was in passed for the rejectUnauthorized parameter, no error was returned and connections to servers with an expired certificate would have been accepted. It was classed as low severity.

**READ** Popular Node.js package vulnerable to command injection attacks

Finally, a use-after-free flaw (CVE-2021-22930) which could allow an attacker to exploit memory corruption to change process behavior was included as a follow-up fix after previous mitigations did not completely resolve the issue.

All users should upgrade to the latest version of Node.js to be protected against the flaws. More information can be found at the Node.js blog.

## Injection attacks reloaded

Latest Posts

Exercise caution
Wodify vulnerabilities allow attacke
steal gym payments, extract memb

Related-domain attacks
Hundreds of high-traffic web doma
vulnerable to exploitation

DNS disruption
Exhaustive study puts China's infa
Great Firewall under the microscop

The security advisory was released on the same day that a research paper (PDF) related to this topic was published.

Researchers Philipp Jeitner and Haya Shulman are due to discuss their work at the Usenix conference, which is held virtually today.

In the research, titled ‘Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS’, they demonstrate “a new method to launch string injection attacks by encoding malicious payloads into DNS records”.

**RELATED** Potential remote code execution vulnerability uncovered in Node.js apps

Vulnerabilities Research RCE XSS Open Source Software DevSecOps Secure Development Events Industry News DNS Cyber-attacks API Denial of Service JavaScript Supply Chain Attacks Hacking News Hacking Techniques Authentication

**Jessica Haworth**

@JesscaHaworth

## Related stories

### Exercise caution

Wodify vulnerabilities allow attackers to steal gym payments, extract member data

13 August 2021

### Related-domain attacks

Hundreds of high-traffic web domains vulnerable to exploitation

12 August 2021

### DNS disruption

Exhaustive study puts China’s infamous Great Firewall under the microscope

12 August 2021

### Node.js vulnerab could allow remc domain hijackin

12 August 2021

**Burp Suite**

Web vulnerability scanner
Burp Suite Editions
Release Notes

**Vulnerabilities**

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

**Customers**

Organizations
Testers
Developers

**Company**

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

**Insights**

Web Security Academy
Blog
Research
The Daily Swig

PortSwigg

Follow us