Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Several bugs in Node.js lead to Remote Code Execution

Date of Publication	Admiralty Code	TA Number
12 July, 2022	A2	TA2022143

Summary

Node.js has released several fixes for vulnerabilities in the JavaScript runtime environment, which could lead to arbitrary code execution, HTTP request smuggling, DNS rebinding vulnerability and other bugs.

CVE Table

CVE	NAME	PATCH
CVE-2022-32213	HTTP Request Smuggling - Flawed Parsing of Transfer-Encoding	✓
CVE-2022-32214	HTTP Request Smuggling - Improper Delimiting of Header Fields	✓
CVE-2022-32215	HTTP Request Smuggling - Incorrect Parsing of Multi-line Transfer-Encoding	✓
CVE-2022-32212	DNS rebinding	✓
CVE-2022-32223	DLL Hijacking on Windows	✓
CVE-2022-32222	openssl.cnf security bypass	✓
CVE-2022-2097	OpenSSL - AES OCB fails to encrypt	✓

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0005** Defense Evasion	**T1518** Software Discovery	**TA0043** Reconnaissance
T1574.001 Hijack Execution Flow: DLL Search Order Hijacking	**T1574.002** Hijack Execution Flow: DLL Side-Loading	**T1583.002** Acquire Infrastructure: DNS Server	**TA0042** Resource Development
TA0003 Persistence	**TA0001** Initial Access	**T1190** Exploit Public-Facing Application	**TA0004** Privilege Escalation

Technical Details

#1

Node.js fixed multiple HTTP request smuggling vulnerabilities that occur due to improper handling of multi-line Transfer-Encoding headers and improper delimiting of header fields

#2

High severity vulnerability, DNS rebinding, could allow a remote attacker to execute arbitrary code on the system due to 'IsIPAddress' field fails to properly check whether an IP address is invalid or not. By monitoring the victim's DNS server or spoofing their responses, an attacker could exploit this vulnerability to bypass the IsAllowedHost check and run arbitrary code on the system.

#3

Node.js uses an OpenSSL configuration file by specifying the environment variable OPENSSL_CONF that leads to DLL hijacking vulnerability. A local attacker can gain elevated privileges on the system using a specially crafted DLL file caused by the DLL search order hijacking of 'providers.dll' file.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-32213 CVE-2022-32214 CVE-2022-32215	Node.js 14.x, 16.x, 18.x and llhttp 2.15, 6.0.7	cpe:2.3:a:llhttp:llhttp:*:*:*:*:*:node.js:*:*,cpe:2.3:a:node_js_foundation:nodejs:*:*:*:*:*:*:*:*	CWE-444
CVE-2022-32212	Node.js 14.x, 16.x, 18.x	cpe:2.3:a:node_js_foundation:nodejs:*:*:*:*:*:*:*:*	CWE-350
CVE-2022-32223	Node.js 16.x and 14.x	cpe:2.3:a:node_js_foundation:nodejs:*:*:*:*:*:*:*:*	CWE-427
CVE-2022-32222	Node.js 18.x	cpe:2.3:a:node_js_foundation:nodejs:*:*:*:*:*:*	-
CVE-2022-2097	Node.js 14.x, 16.x and 18.x	cpe:2.3:a:node_js_foundation:nodejs:*:*:*:*:*:*:*:*	CWE-311

Patch Links

https://nodejs.org/en/blog/release/v14.20.0/
https://nodejs.org/en/blog/release/v16.16.0/
https://nodejs.org/en/blog/release/v18.5.0/

References

https://nodejs.org/en/blog/vulnerability/july-2022-security-releases/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 12, 2022 • 11:30 PM

More at www.hivepro.com