Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0492

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Node.js

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Node.js heeft meerdere kwetsbaarheden verholpen in versies 22.x, 24.x en 26.x, waaronder in de HTTP/2-implementatie, HTTPS-servermodule, TLS-handling en proxy error handling.

Duiding

Verschillende kwetsbaarheden in Node.js kunnen leiden tot informatielekken, geheugenfouten en serveruitval. Vooral omgevingen met HTTP/2, HTTPS en TLS worden geraakt.

- Proxy-authenticatie: uitlekken van inloggegevens via foutmeldingen.
- HTTP/2: buffer overflow, geheugenlekken, overbelasting en servercrashes.
- Bestandsbewaking: omzeilen van toegangsbeperkingen op macOS en Windows.
- zlib: dienstverstoring door foutieve verwerking van datastromen.
- HTTPS-server: geheugenfouten waardoor gevoelige gegevens, waaronder TLS-privésleutels, kunnen uitlekken.
- TLS 1.2: omzeilen van authenticatie met clientcertificaten.
- TLS-sessies: onjuist hergebruik van sessies met verschillende certificaatinstellingen.

Oplossingen

Node.js heeft updates uitgebracht in versies 22.23.0, 24.17.0, 24.18.0 en 26.x om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://nodejs.org/en/blog/vulnerability/november-2026-security-releases

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-48615	7.5 HIGH
CVE-2026-123828	5.9 MEDIUM
CVE-2026-123829	2.5 LOW
CVE-2026-123862	5.9 MEDIUM
CVE-2026-123863	8.2 HIGH
CVE-2026-123864	8.1 HIGH
CVE-2026-123865	7.5 HIGH
CVE-2026-123866	7.5 HIGH
CVE-2026-123867	4.2 MEDIUM
CVE-2026-123868	5.9 MEDIUM
CVE-2026-123871	6.2 MEDIUM
CVE-2026-123872	8.1 HIGH
CVE-2026-123874	7.5 HIGH
CVE-2026-123875	5.9 MEDIUM
CVE-2026-123877	6.8 MEDIUM
CVE-2026-126051	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-248	Uncaught Exception
CWE-295	Improper Certificate Validation
CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
CWE-416	Use After Free

CWE	Beschrijving
CWE-476	NULL Pointer Dereference
CWE-617	Reachable Assertion
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-825	Expired Pointer Dereference
CWE-1230	Exposure of Sensitive Information Through Metadata
CWE-1265	Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls

Getroffen producten

Open Source
Node.js

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.