SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

RAPORT TEHNIC DE SECURITATE

Node2Shell
Executare de cod prin Brotli

CVE-2026-111497

1 Sumar executiv

Se recomandă actualizarea urgentă a instanțelor Node.js care prelucrează date Brotli nefiabile, cu prioritate pentru serviciile publice. CVE-2026-111497 poate permite coruperea memoriei, divulgarea datelor procesului, indisponibilitate și executarea de cod la distanță.

ELLIO a raportat trafic de exploatare observat la 26 octombrie 2026 și validarea în laborator a executării de cod pe un build vulnerabil. Observația furnizorului justifică prioritizarea remedierii; ea nu confirmă compromiterea unei infrastructuri locale.

Element	Constatare pentru decizia operațională
Identificator și denumiri	CVE-2026-111497; Node2Shell, întâlnită și ca HTTP2Shell sau Broccoli2Shell. Denumirile nu limitează problema la HTTP/2.
Severitate	Google CNA: Critică, CVSS v4.0 9,2. Proiectul Node.js: Ridicată. Evaluările sunt prezentate separat.
Condiție de expunere	Date Brotli controlate de atacator ajung efectiv la un decodor afectat; simpla instalare a Node.js sau primirea unei cereri HTTP nu demonstrează această cale.
Suprafețe relevante	Corpuri de cerere decomprimate de middleware, răspunsuri externe procesate de clienți HTTP și utilizarea directă a API-urilor Brotli. Secțiunea 3 detaliază verificarea.
Praguri Node.js	22.23.4, 24.22.1 și 26.12.1, ori versiuni ulterioare remediate din ramura folosită.
Verificare esențială	Se verifică runtime-ul activ și proveniența pachetului. Numărul Brotli 1.2.0, luat izolat, nu stabilește dacă Node.js este remediat.
Limită metodologică	Analiză a surselor publice și a modificărilor de cod. Nu au fost efectuate scanări, teste de exploatare ori verificări în infrastructura instituției.

Acțiuni prioritare

- Inventarierea tuturor binarelor Node.js, imaginilor container, replicilor și aplicațiilor care includ runtime-ul; identificarea căilor de decomprimare și a responsabililor tehnici.
- Instalarea runtime-ului remediat, reconstruirea și redistribuirea livrabilelor, apoi înlocuirea proceselor și replicilor vechi. Ramurile fără suport necesită migrare sau o corecție explicit confirmată de furnizor.
- Analiza retrospectivă a cererilor Brotli, a răspunsurilor externe, a căderilor procesului și a activității neautorizate. Suspiciunile se gestionează distinct de tichetul de actualizare.

2 Fișa tehnică a vulnerabilității

Câmp tehnic	Detaliu
Identificator	CVE-2026-111497; produsul upstream este Google Brotli, integrat și în Node.js.
Descriere succintă	Un flux Brotli invalid poate determina o scriere în afara bufferului decodorului și alterarea memoriei procesului.
Componentă afectată	Decodorul nativ Brotli, în special c/dec/decode.c. În build-urile oficiale Node.js, codul este inclus sub deps/brotli; nu este o simplă dependență npm.
Tipul vulnerabilității	CWE-787 — Out-of-bounds Write; CWE-252 — Unchecked Return Value, conform Google CNA.
Condiții de exploatare	Date comprimate controlate de atacator, o cale de decomprimare activă și un decodor afectat. Vectorul publicat indică acces de rețea, fără privilegii și fără interacțiunea utilizatorului.

Câmp tehnic	Detaliu
Mod de exploatare	Prelucrarea unui flux construit special corupe starea decodorului; transformarea în RCE depinde de build, arhitectură și contextul procesului. Nu fiecare intrare invalidă produce un shell.
Cauza tehnică	Un block switch invalid era tratat ca o nevoie temporară de date suplimentare. Corecția separă eroarea de format de situația în care intrarea este incompletă.
Consecințe	RCE cu drepturile serviciului, căderea procesului și posibila divulgare a memoriei. Accesul la alte sisteme depinde de identitățile și permisiunile disponibile procesului.
Dovezi publice	Demonstrație RCE pe Linux arm64 publicată de Imperva; ELLIO raportează reproducere pe x86-64 și trafic de exploatare. Sunt rezultate ale furnizorilor, nu teste efectuate în acest raport.
Detectare și monitorizare	Corelarea datelor Brotli primite sau descărcate cu erori, restarturi și activitate de proces. O potrivire de antet ori o eroare izolată nu confirmă exploatarea.

3 Mecanismul și suprafețele de atac

Cum apare coruperea memoriei

La o tranziție de bloc nevalidă, decodorul vulnerabil putea continua să solicite intrare în loc să oprească procesarea cu eroare de format. Datele erau adăugate într-un buffer intern de opt octeți. Continuarea procesării în această stare permitea depășirea limitei bufferului și coruperea memoriei.

Commitul `upstream 0ed4268a4401abcb4472096340477cf4af7d1a2b` introduce propagarea distinctă a erorii de format pentru `block switch`. Intrarea invalidă este respinsă, în loc să fie interpretată ca un flux temporar incomplet. Acesta este mecanismul de remediere urmărit în analiză; nu au fost rulate payloaduri.

Căi prin care datele ajung la decodor

Cale	Condiție de expunere	Ce trebuie verificat
Cereri către aplicație	Middleware-ul decomprimă un corp cu Content-Encoding: br.	Parserul efectiv, ordinea middleware-urilor și accesibilitatea rutelor. Un control de acces ulterior decomprimării nu protejează acel pas.
Răspunsuri externe	Un client, inclusiv `fetch()`, primește și decodează un răspuns Brotli nefiabil.	Previzualizări de linkuri, importuri, webhookuri și servicii care descarcă URL-uri influențate de terți.
Apel direct al bibliotecii	Aplicația folosește funcții Brotli din node:zlib pe date externe.	Cod, dependențe și procesare de fișiere sau fluxuri, chiar fără endpoint public direct.

Ce stabilesc demonstrațiile publice

Imperva a demonstrat execuție pe imaginea oficială Node.js 24.22.0 Linux arm64, prin `fetch()` și `parsere` de cereri. Au fost testate configurații punctuale cu Express 5 și body-parser 2; 24.22.1 a respins aceleași intrări. Aceste pachete descriu căi de acces la runtime, nu mută defectul din biblioteca nativă în framework.

Un server `node:http` nu decomprimă automat orice corp primit. De aceea, inventarul versiunilor trebuie completat cu analiza fluxului de date. Absența unei rute publice care acceptă Brotli nu exclude calea unui răspuns extern sau a unei prelucrări directe.

4 Versiuni afectate și remediate

Build-uri oficiale Node și ramuri în suport

Ramură	Versiuni anterioare afectate	Prag remediat
22.x	22.x înainte de 22.23.4	22.23.4 sau ulterior
24.x	24.x înainte de 24.22.1	24.22.1 sau ulterior
26.x	26.x înainte de 26.12.1	26.12.1 sau ulterior
20.x, 23.x, 25.x	Ramuri upstream ieșite din suport la data raportului.	Migrare la o ramură în suport; verificarea oricărui backport comercial ori al distribuției.

Pragurile se aplică build-urilor oficiale. Ramurile mai vechi și produsele care includ un runtime propriu se inventariază separat; lipsa unei ramuri din tabel nu constituie o declarație de neafectare.

Biblioteca Google Brotli și corecțiile pe ramuri

Ramură Brotli	Interval afectat în datele CNA	Prima versiune remediată
1.0.x	1.0.3–1.0.9	1.0.10
1.1.x	1.1.0	1.1.1
1.2.x	1.2.0	1.2.1

5 Exploatare observată și indicatori publicați

Cronologia dovezilor publice

Dată	Dovadă și limită
21.10.2026	Node.js publică actualizările de securitate pentru ramurile întreținute.
22.10.2026	Imperva publică demonstrația RCE și comparația cu runtime-ul remediat. Rezultatele sunt de laborator.
23.10.2026	Evaluarea CISA ADP din înregistrarea CVE indică Exploitation: none; este o constatare datată.
26.10.2026 15:08 UTC	ELLIO raportează o cerere de exploatare în senzorii proprii, destinată Node.js 24.22.0 x86-64. Aceasta este observația rețelei furnizorului.

Fluxul public CISA KEV consultat, cu data de actualizare 26 octombrie 2026, nu include identificatorul. Această absență și evaluarea din 23 octombrie nu anulează observația ulterioară ELLIO și nu sunt criterii pentru amânarea actualizării.

Indicatori și artefacte pentru corelare

Indicator	Interpretare
94[.]154[.]43[.]7	Adresă sursă atribuită cererii de exploatare de ELLIO; se caută în retenția relevantă.
node2shell-check	Identificator al unui verificator de expunere observat înaintea exploatării. Semnal de recunoaștere, nu dovadă de RCE.
Content-Encoding: br	Context de decomprimare. Antet legitim, insuficient pentru a atribui o cerere unei campanii.

SHA-256 al corpului HTTP observat de ELLIO, cu dimensiunea de 23.069.983 octeți. Este hash-ul acelui eșantion de trafic, nu al unui fișier instalat pe gazdă.

7fcbdaaecd4419e2930927844f3b772668204737a4e7602a2290c991c93c5c4b

Cum se folosesc indicatorii

Se corelează timpul, sursa, cererea, runtime-ul și telemetria gazdei. Dimensiunea și hash-ul unui singur eșantion nu acoperă toate variantele. Lipsa potrivirilor nu exclude exploatarea. Un antet, un scaner sau o conexiune dintr-o adresă raportată nu confirmă, singure, succesul atacului.

RCE observat în testele publice este specific build-urilor și condițiilor validate. Un payload care nu reușește pe un alt build nu dovedește că acel build este remediat. Confirmarea unui incident local necesită dovezi proprii.

6 Detectare și monitorizare

Se recomandă corelarea evenimentelor de la proxy/WAF, aplicație, sistemul de operare și EDR. Se includ atât cererile primite, cât și răspunsurile externe descărcate. Regulile următoare sunt propuneri de investigație, nu semnături care confirmă singure CVE-2026-111497.

Sursă de telemetrie	Semnal urmărit	Verificare de triere
Proxy și WAF	Cereri br neobișnuite, creșteri de volum, resetări și erori corelate.	Ruta, sursa, acțiunea efectivă a regulii și limitele de inspecție; nu se păstrează inutil conținut sensibil.
Client HTTP și aplicație	Răspuns extern comprimat urmat de eroare sau cădere.	URL-ul și lanțul de redirecționări, procesul care consumă corpul și contextul de decomprimare.
Sistem și orchestrator	SIGSEGV, crash-uri, restarturi repetate, creșteri ale CPU sau întârzieri.	Se corelează cu traficul și schimbările aprobate; căderea poate avea și cauze legitime.
EDR și audit de procese	Node.js lansează un shell, utilitare ori conexiuni neobișnuite.	Identitate, arbore de procese, argumente și destinații; se exclud sarcinile autorizate.
Fișiere și artefacte	Modificări neaprobate, descărcări și apariția unor core dump-uri.	Integritate, proveniență și drepturi de acces. Core dump-urile pot conține date și secrete din memorie.

Mapare MITRE ATT&CK pentru investigație

Tehnică	Aplicare condițională
T1190 Exploit Public-Facing Application	Pentru acces prin exploatarea unei aplicații publice; nu acoperă automat orice consum de răspuns extern. [18]
T1059.004 Unix Shell	Dacă dovezile arată executarea unui shell după compromiterea procesului. [18]
T1105 Ingress Tool Transfer	Numai dacă este observat un transfer ulterior de unelte sau payloaduri. Nu este un efect implicit al CVE. [18]

7 Inventariere și verificări locale

Exemplele sunt verificări locale de citire. Se adaptează la sistem și se rulează în mediul aplicației ori al containerului relevant. Nu trimit cereri de exploatare.

Identificarea binarului și a versiunii

```
command -v node
node --version
node -p 'JSON.stringify({node:process.version,arch:process.arch,
  execPath:process.execPath,brotli:process.versions.brotli})'
ps -eo pid,ppid,user,lstart,args --forest | rg 'node|pm2'
```

process.execPath și process.versions descriu binarul invocat. Acesta poate diferi de cel al serviciului, al unui manager de versiuni ori al unui container. Se corelează PID-ul serviciului cu executabilul său; pe Linux, /proc/PID/exe poate ajuta la această identificare, folosind PID-ul real în locul marcajului.

Dependențe și căi de decomprimare

```
npm ls express body-parser @koa/bodyparser --all
rg -n 'brotliDecompress|createBrotliDecompress|Content-Encoding|express\.json|express\.raw' \
  src package.json package-lock.json
```

Comenzile se execută din proiectul disponibil, cu directoare adaptate. Inventarul npm ajută la identificarea căilor de acces, însă nu dovedește corectarea bibliotecii native din Node.js. O căutare în surse nu acoperă automat codul generat, toate dependențele sau integrările externe.

Jurnale și starea serviciului pe Linux

```
journalctl -u NUME_SERVICIU --since '2026-10-21 00:00:00' --no-pager
coredumpctl list node
ss -tpn
```

NUME_SERVICIU este un marcaj de înlocuit. Data este un punct de pornire, nu începutul garantat al expunerii. Se verifică retenția relevantă și fusurile orare; lipsa unor rezultate nu certifică inexistența exploatării. Comenzile disponibile diferă între gazde și containere. Nu se exportă public dump-uri sau jurnale sensibile.

8 Remediere și reducerea expunerii

Acțiuni pentru remedierea completă

- Se selectează pragul remediat din ramura utilizată sau un pachet pentru care furnizorul confirmă explicit corecția. Pentru ramuri fără suport se planifică migrarea.
- Se actualizează gazda sau imaginea de bază, se reconstruiesc aplicațiile care includ runtime-ul și se face redeploy. Se înlocuiesc toate procesele, nodurile și replicile care rulează binarul vechi.
- Se verifică versiunea efectiv pornită, compatibilitatea și prelucrarea normală a datelor. Se păstrează dovezile și se urmăresc erorile după schimbare; criteriile sunt în secțiunea 9.

Controale temporare până la actualizare

Măsură	Aplicare și limită
Filtrarea cererilor Brotli	Se resping cererile cu Content-Encoding: br înainte ca octeții să ajungă la parserul afectat. Se acoperă toate rutele și accesul direct la origin. Nu acoperă răspunsurile externe.
Decomprimarea în middleware	Se poate dezactiva temporar funcția de inflate a parserelor, dacă integrarea permite. Se testează impactul asupra tuturor codificărilor și rutelor utilizate.
Răspunsuri externe	Se limitează sursele nefiabile și se controlează codificarea înainte de decodor, printr-un client sau intermediar potrivit. Solicitarea Accept-Encoding: identity nu garantează că un server malițios o respectă.
WAF și limite de trafic	Se verifică protecția specifică și acțiunea de blocare. Limitele de corp, rată și timp reduc anumite scenarii; dimensiunea unui payload observat nu este un prag universal de siguranță.
Privilegii și secrete	Cont cu drepturi minime, segmentare și acces minim la secrete. Se protejează dump-urile și se limitează retenția lor. Aceste măsuri reduc impactul, fără a corecta decodorul.

10 Surse și referințe

Consultate la 27 octombrie 2026. Datele tehnice și observațiile publice sunt atribuite surselor. Prioritățile, corelările și criteriile de acceptare sunt recomandări ale raportului. Legăturile de mai jos sunt către materiale publice.

[1] Cyber Kendra — tema indicată
Node2Shell Exploited in the Wild

[2] Proiectul Node.js
October 21 2026 Security Releases — CVE-2026-111497

[3] CVE Program — Google CNA și CISA ADP
CVE-2026-111497 — intervale structurate și CVSS

[4] Proiectul Node.js
Node.js 22.23.4 — lansare de securitate

[5] Proiectul Node.js
Node.js 24.22.1 — lansare de securitate

[6] Proiectul Node.js
Node.js 26.12.1 — lansare de securitate

[7] Google Brotli — modificarea upstream
Detect and report invalid stream earlier — commit 0ed4268a

[8] Google Brotli — lansări cu corecția
v1.0.10 | v1.1.1 | v1.2.1

[9] Imperva Threat Research — 22.10.2026
Node2Shell From Brotli Data to Remote Code Execution

[10] ELLIO Threat Research — actualizare 26.10.2026
RCE on stock Node.js builds — observații și indicatori

[11] Node.js Release Working Group
Calendarul oficial al ramurilor

[12] Debian Security Tracker
CVE-2026-111497 — bibliotecă de sistem și backporturi

[13] Documentația Node.js
process.execPath și process.versions

[14] Sursele oficiale Node.js — antetul versiunii Brotli
v24.22.0 | v24.22.1

[15] Express — body-parser
README — opțiunile de decomprimare și inflate

[16] Node.js — decomprimare și client HTTP
API zlib | Undici în v24.22.1

[17] CISA — catalogul KEV public
Fluxul JSON oficial — consultat la 27.10.2026

[18] MITRE ATT&CK — mapare condițională
T1190 | T1059.004 | T1105

[19] FIRST
CVSS v4.0 Specification Document

Modelul de structură și aranjare în pagină indicat de beneficiar
Raport tehnic STISC — exemplarul public furnizat