नेपाल सरकार

प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय

सूचना प्रविधि तथा विद्युतीय शासन कार्यालय

राष्ट्रिय साइबर सुरक्षा केन्द्र

सिंहदरबार, काठमाडौं

Advisory Number: NCSC-1146-115-05

मितिः २०८३/०७/११

साइबर सुरक्षा एडभाइजरी

हालै Node.js Runtime मा Node2Shell (CVE-2026-111497) लगायतका गम्भीर सुरक्षा कमजोरीहरू पहिचान भएका छन्। यस्ता कमजोरीको दुरुपयोग भएमा सम्बन्धित प्रणालीमा अनधिकृत पहुँच प्राप्त हुने, सेवा अवरुद्ध हुने तथा प्रणालीमा चलिरहेका कार्यहरूमा अनधिकृत नियन्त्रण कायम हुन सक्ने जोखिम रहन्छ। यसबाट बच्न देहाय बमोजिमका सुरक्षा उपायहरू तत्काल अवलम्बन गर्नुहुन सम्बन्धित सबै निकाय तथा प्रणाली सञ्चालकहरूमा अनुरोध छ।

१. सम्बन्धित निकायका प्रणाली तथा वेब एप्लिकेसनमा प्रयोग भएको Node.js Runtime को version जाँच गरी निम्न version मा अपग्रेड गर्नुहोस।

Current Version (Status)	**Required Action**
Node.js 26.x (Current LTS)	Upgrade to **26.12.1 or later**.
Node.js 24.x (LTS)	Upgrade to **24.22.1 or later**.
Node.js 22.x (LTS)	Upgrade to **22.23.4 or later**. Node.js 22.x reaches EOL on April 30, 2027. It is recommended to plan migration to Node.js 24 LTS or 26 LTS.
Node.js 25.x, 23.x, 20.x, 18.x or older (End-of-Life)	These End-of-Life versions do not receive the required security fixes. Upgrade to a supported, secure release line, preferably **Node.js 24 LTS or 26 LTS**, after compatibility testing.

Advisory Number: NCSC-1146-115-05 मितिः २०८३/०७/११

२. एकीकृत डाटा व्यवस्थापन केन्द्रमा होस्ट भएका प्रणालीहरुका सन्दर्भमा Runtime अद्यावधिक तथा सुरक्षा प्याच कार्यान्वयनका सम्बन्धमा थप प्राविधिक सहजीकरण आवश्यक भएमा यस केन्द्रका कम्प्युटर अधिकृत श्री आशिष भट्ट (सम्पर्कः ९८४४६८२७४२) तथा एकीकृत डाटा व्यवस्थापन केन्द्र (IDMC) का कम्प्युटर अधिकृत श्री मुकेश कुशवाहा (सम्पर्कः ९८६१५९२३०१) सँग आवश्यक समन्वय गर्नुहुन अनुरोध छ।

३. अद्यावधिक कार्य सम्पन्न भएपछि सम्बन्धित प्रणालीको सञ्चालन अवस्था तथा सुरक्षा परीक्षण गरी अद्यावधिक सफल भएको सुनिश्चित गर्नुहोस्। सुरक्षा कमजोरीको सम्भावित दुरुपयोग भएको आशङ्का भएमा सम्बन्धित प्रणालीका Log तथा अन्य डिजिटल प्रमाणहरू सुरक्षित राखी तत्काल यस केन्द्रलाई जानकारी गराउनुहोस्।

Node.js अपग्रेड गर्ने तरिका

Step 1: Check the currently installed version

Run the following commands on each server or host running Node.js:

```
node --version
which -a node
```

Step 2: Upgrade Node.js

Upgrade to the latest patched release in the supported Node.js LTS. Use the official download page to obtain the appropriate installer or binary:

https://nodejs.org/en/download

For systems using Docker, update the base image to a patched Node.js image and rebuild the application image.

If you use `nvm`, upgrade can be done with following commands:

```
nvm install --lts
```

```
nvm use –lts
```

Step 3: Rebuild and redeploy the application

- Rebuild application artifacts, containers, and serverless functions using the patched runtime.
- Redeploy the application and restart the affected services.
- Ensure that no old or bundled Node.js binaries remain in use.

Step 4: Verify the upgrade

Run the following commands:

```
node --version
node -p "process.execPath"
```

Confirm that the running application uses the patched Node.js runtime. Test application functionality and review logs for errors after deployment.

Step 5: Apply additional security measures

- Review applications that decompress Brotli-encoded requests or process responses from untrusted URLs.
- Review DNS resolution, outbound request validation, and TLS certificate verification.
- Check for signs of exploitation and preserve relevant logs.
- If compromise is suspected, isolate the affected system as appropriate, notify the security team, and rotate potentially exposed credentials.

Verify with `npm audit` or operating system package updates and confirm the patched version against the official Node.js security releases before deployment.