



CYBERSECURITY ADVISORY

Multiple vulnerabilities in Node.js

Severity: High | Highest vendor rating

Overview

All organisations and individuals in Kenya operating systems built on Node.js are advised to identify affected runtimes and apply the security updates promptly. This includes public institutions, county governments, businesses, critical infrastructure operators, educational institutions, developers and service providers. The advisory covers systems operated directly or managed by third parties, including cloud and hosted environments.

Node.js has released fixes for ten vulnerabilities in the 22.x, 24.x and 26.x release lines, including remote code execution through the Brotli decoder, TLS certificate validation bypasses and a DNS name-handling flaw. Exposure depends on the functionality used by each application.

Principal high severity vulnerabilities

CVE	Vulnerability	Affected release lines
CVE-2026-111497	Brotli decoder out-of-bounds write permitting remote code execution	22.x, 24.x, 26.x
CVE-2026-105482	DNS name truncation when a name contains a NUL character	22.x, 24.x, 26.x
CVE-2026-105483	TLS hostname verification bypass involving fullwidth digits	24.x, 26.x
CVE-2026-106069	TLS hostname verification bypass involving hosts interpreted as IP addresses	22.x, 24.x, 26.x

The release also fixes medium- and low-severity issues involving HTTP connections, certificate validation, repeated random values in startup snapshots, ZIP handling and filesystem permissions.

Affected and fixed versions

Node.js branch	Affected versions	Fixed version
22.x	Earlier than 22.23.4	22.23.4
24.x	Earlier than 24.22.1	24.22.1
26.x	Earlier than 26.12.1	26.12.1

Unsupported releases should be migrated to a supported, patched version.

Recommended actions

1. Upgrade affected Node.js runtimes promptly, prioritising exposed services and applications processing untrusted compressed content.
2. Inventory Node.js runtimes across websites, portals, APIs, internal applications, servers, containers, development environments and build systems.
3. Rebuild and redeploy container images and applications that bundle their own runtime. Restart services and verify the version used by each running application.
4. Require hosting providers and vendors responsible for managed services or packaged applications to confirm affected systems and patch completion.
5. Review unexpected process crashes, child processes, file changes and outbound connections. Preserve evidence and investigate suspicious activity.

Updating npm packages or running npm audit alone does not replace updating the Node.js runtime.

Reference

Node.js official security release <https://nodejs.org/en/blog/vulnerability/october-2026-security-releases>