

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-7808

Summary

CVE-2026-7808 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. justhtml before 1.16.0 contains multiple HTML sanitization bypass issues that can allow active/dangerous content (e.g., script or style) to survive sanitization, potentially leading to cross-site scripting. The issues primarily affect advanced usage rather than the default JustHTML(..., sanitize=True) path for ordinary parsed HTML: mutating or reusing sanitization policy objects (including exported defaults) could weaken later sanitization; programmatic DOM input to sanitize()/sanitize_dom() could miss mixed-case tag names (e.g., ScRiPt, StYIE); crafted programmatic doctype names could serialize into active markup; and custom policies preserving SVG or MathML could allow animation elements, presentation attributes with external url(...) references, or DOM trees mislabeled as namespace="html" to bypass foreign-content checks. Fixed in 1.16.0.

What we know

- **CVE:** CVE-2026-7808
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.