TS PARTNERS

|630 Freedom Business Center Dr., Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

October 19, 2022

Text4Shell: CVE-2022-42889 in Apache Commons Text

A vulnerability in the Apache Commons Text library indicates that attackers can perform remote code execution (RCE). This new vulnerability is being analyzed currently by NIST and others.

NIST - Current Description [https://nvd.nist.gov/vuln/detail/CVE-2022-42889].

Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.text.lookup.StringLookup that performs the interpolation.

Starting with version 1.5 and continuing through 1.9, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used.

Users are recommended to upgrade to Apache Commons Text 1.10.0, which disables the problematic interpolators by default.

TS Partners' Research

TSP Software Engineering has reviewed available information and determined the vulnerability does not affect either the TranStar or LinkStar application.

TranStar

TranStar does not maintain references to Apache Commons Text Library that could cause it to be affected.

LinkStar

While LinkStar does maintain 'apache commons-text: 1.3', version 1.3 is not marked as a vulnerable Apache build and the reported problem only affects builds 1.5 to 1.9.

Given this information, there is no need for a remediation plan or upgrades to any of the files in the software.

Mitigation Recommendations (beyond TS Partners' applications that are unaffected)
If your firm identifies a vulnerable version of Apache Commons Text (1.5-1.9), upgrade the library to the patched version (1.10) as soon as possible.

For questions regarding Policy, contact CEO or COO

Last Review: October 18, 2022
Last Revision: October 19, 2022