Security Advisory 2022-072

Apache Commons Text Vulnerability

October 19, 2022 — v1.0

TLP:CLEAR

History:

- *19/10/2022 — v1.0 – Initial publication*

Summary

A vulnerability, tracked as **CVE-2022-42889** with a CVSS score of **9.8** was found in *Apache Commons Text* packages in versions 1.5 through 1.9. The affected versions allow an attacker to benefit from a variable interpolation process contained in Apache Commons Text, which can cause properties to be dynamically defined. Server applications are vulnerable to remote code execution (RCE) and unintentional contact with untrusted remote servers [1].

Technical Details

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. These lookups are: - `script` - execute expressions using the JVM script execution engine (`javax.script`) - `dns` - resolve dns records - `url` - load values from urls, including from 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 [2, 3].

Affected Products

- Apache Commons Text version 1.5 to 1.9

Recommendations

CERT-EU recommends upgrading to Apache Commons Text 1.10.0.

References

[1] https://vulners.com/redhatcve/RH:CVE-2022-42889

[2] https://nvd.nist.gov/vuln/detail/CVE-2022-42889#vulnCurrentDescriptionTitle

[3] https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om