OUTBREAK ALERTS

Apache Text4shell Vulnerability

So-called as Text4Shell but not near yet to Log4Shell

https://blogs.apache.org/security/entry/cve-2022-42889
CVEs: CVE-2022-42889, CVE-2022-33980

A vulnerability on Apache Commons Text library that can allow the attacker to do a Remote Code Execution (RCE) via its interpolation. FortiGuard has added protections throughout the Security Fabric to safeguard its customers from possible attacks.

Background

Apache Commons Text is a library for performing various text operations with values looked up through interpolators. Such examples of text operations are escaping, calculating string differences, and substituting placeholders.

According to the Apache blog, the Apache Common Text issue is different from Log4Shell (CVE-2021-44228) because the affected method is explicitly intended to perform string interpolation. Applications that uses the library is less likely to inadvertently pass untrusted input without proper validation.

Announced

13 Oct, 2022: The Apache Commons Text team disclosed CVE-2022-42889.
https://lists.apache.org/thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om

Latest Developments

18 Oct, 2022: The Apache Security Team posted a blog.
https://blogs.apache.org/security/entry/cve-2022-42889

21 Oct, 2022: FortiGuard telemetry shows low activity on the vulnerability.

FortiGuard has added IPS, FortiADC WAF and FortiWeb WAF signatures to block any attack attempts leveraging these vulnerabilities to protect our customers. Users are recommended to upgrade vulnerable versions as recommended by the vendor and also properly validate and sanitize any untrusted input as a best practice.

Cyber Kill Chain

Reconnaissance

FortiDeceptor
Lure 3.3+
Deception Lure will divert attacker and its activities related to Apache Text4shell Vulnerability towards FortiDeceptor Decoy

Decoy VM 3.3+
Decoys in the network segment can detect the attack and any lateral movement.

Weaponization

Delivery

FortiDevSec
Vulnerability 22.4.0+
Software Composition Analysis scanner detects Apache Commons Text RCE Vulnerability

Exploitation

FortiGate
IPS 22.418
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

FortiWeb
Web App Security 0.00332
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

FortiSASE
IPS 22.418
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

FortiNDR
IPS 22.418
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

FortiADC
IPS 22.418
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

Web App Security 1.00039
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

FortiProxy
IPS 22.418
Detects and Blocks attack attempts related to Apache Commons Text RCE Vulnerability

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiAnalyzer

Outbreak Detection Version 1.00072
https://fortiguard.fortinet.com/updates/outbreak-detection-service?version=1.00072

Threat Hunting Version 7.0+
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Apache-Commons-Text/ta-p/227450

FortiSIEM

Content Update Version 304
https://help.fortinet.com/fsiem/6-6-2/Online-Help/HTML5_Help/content_updates.htm#Content11

Threat Hunting Version 6.4.0+
https://community.fortinet.com/t5/FortiSIEM/Technical-Tip-Using-FortiSIEM-to-detect-Apache-Commons-Text/ta-p/228600

Additional Resources

Apache Blog	https://blogs.apache.org/security/entry/cve-2022-42889
Openwall Security	https://www.openwall.com/lists/oss-security/2022/10/13/4
Security Week	https://www.securityweek.com/critical-apache-commons-text-flaw-compared-log4shell-not-widespread
Dark Reading	https://www.darkreading.com/application-security/researchers-keep-a-wary-eye-on-critical-new-vulnerability-in-apache-commons-text
Bleeping Computer	https://www.bleepingcomputer.com/news/security/apache-commons-text-rce-flaw-keep-calm-and-patch-away/
The Hacker News	https://thehackernews.com/2022/10/hackers-started-exploiting-critical.html