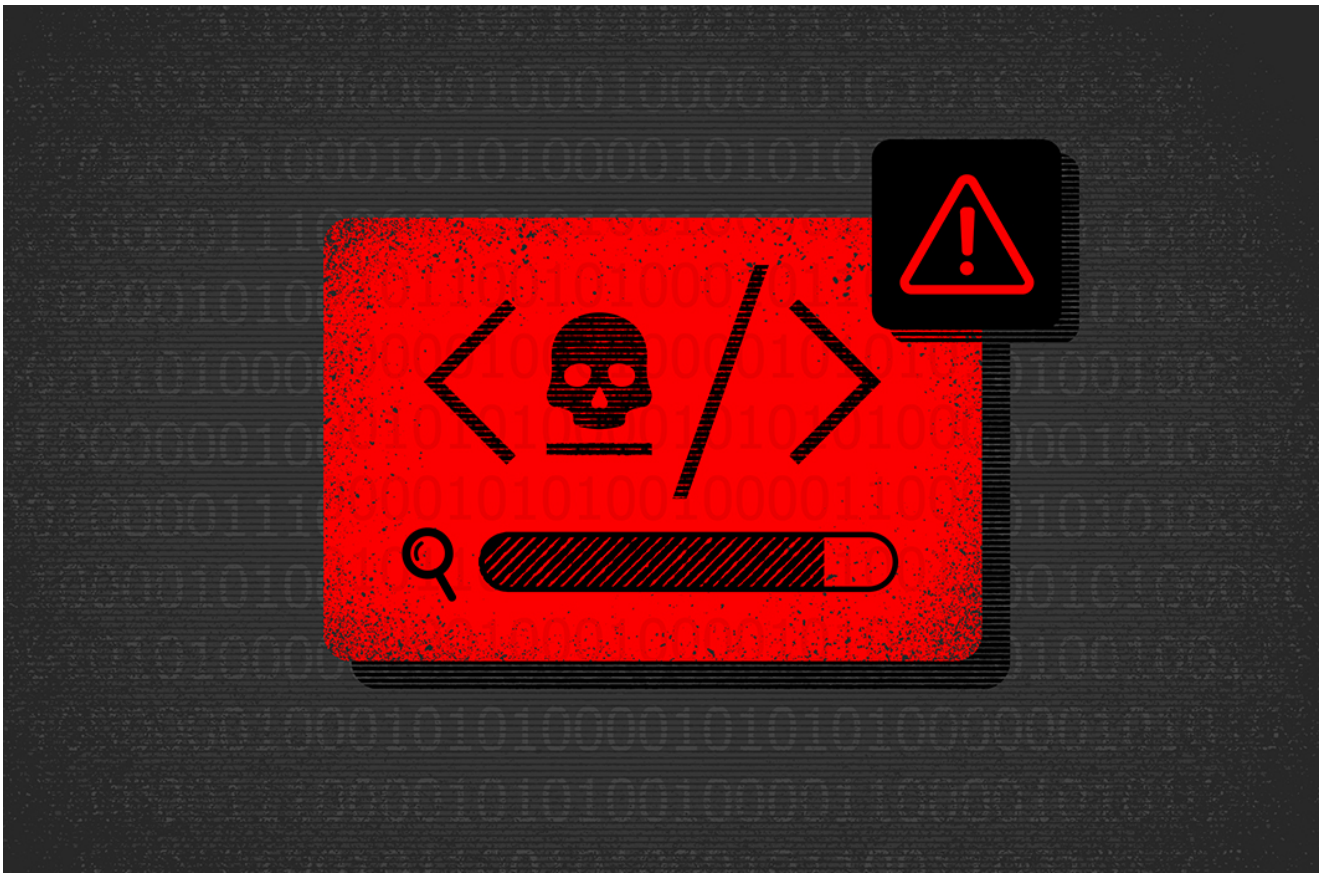
CrowdStrike Launches Free Targeted Log4j Search Tool

crowdstrike.com/blog/free-targeted-log4j-search-tool/

Randy Burton - Ian Barton December 22, 2021



The recently discovered Log4j vulnerability has serious potential to expose organizations across the globe to a new wave of cybersecurity risks as threat actors look to exploit this latest vulnerability to execute their malicious payloads using remote code execution (RCE).

An immediate challenge that every organization faces is simply trying to understand exactly where you have applications that are using this very popular Java library — but you are not facing this challenge alone.

The CrowdStrike Services team has been busy developing a community tool that can be used to quickly scan file systems looking for versions of the Log4j code libraries to help organizations understand what they need to patch in order to mitigate their risk.

The free CrowdStrike tool (dubbed the CrowdStrike Archive Scan Tool, or “CAST”) performs a targeted search by scanning a given set of directories for JAR, WAR, ZIP and EAR files, and then it performs a deeper scan on those file types matching against a known set of checksums for Log4j libraries. We help organizations find any version of the affected Log4j library anywhere on disk, even if it is deeply nested in multiple levels of archive files.

CAST searches for approximately 6,500 SHA256 checksums unique to the known vulnerable releases. It will walk the files or directories scanning inside of ZIP-format archives to find every instance of these. As we developed the tool, we carefully considered the following:

- Be mindful of the resource consumption when running a scan to minimize the impact on end-user systems.
- Intentionally allow a higher number of false-positive results, leaving the decision in the hands of the system owners whether a given result warrants further investigation.
    We may see higher false positives because we identify any trace of vulnerable versions of Log4j, even if the vulnerability has been addressed by removing one or more classes from the deployment.
- The results should be extremely reliable, as they're based on cryptographic checksums.
- Allow use of the tool with pre-indexed (e.g., "locate") file systems to avoid scanning and simply pass the paths to known files on the command line.
    For example, locate -0 *.jar | xargs -0 ./cast
- Provide the ability to tune memory usage — for example:
    - -recursion 0 to disable scanning sub-archives
    - -recursion 1 to scan only 1 sub-archive deep
    - -maxmem 1000000 to limit sub-archive scanning to 1MB (compressed)

The tool is intentionally single-threaded as we have to be conscious of resource consumption and allow users or administrators to manage their own resources. One thread will (in our experience) scan a file system quickly enough. One could scan multiple directories simultaneously by executing multiple copies of the tool, but the file system load would likely cause a noticeable user impact.

Staying true to CrowdStrike's **cross-platform** focus, we developed CAST as a tool that will run on **Windows, Mac and Linux** systems, and we are using the tool in CrowdStrike Services engagements to assist our clients who need support to find Log4j instances.

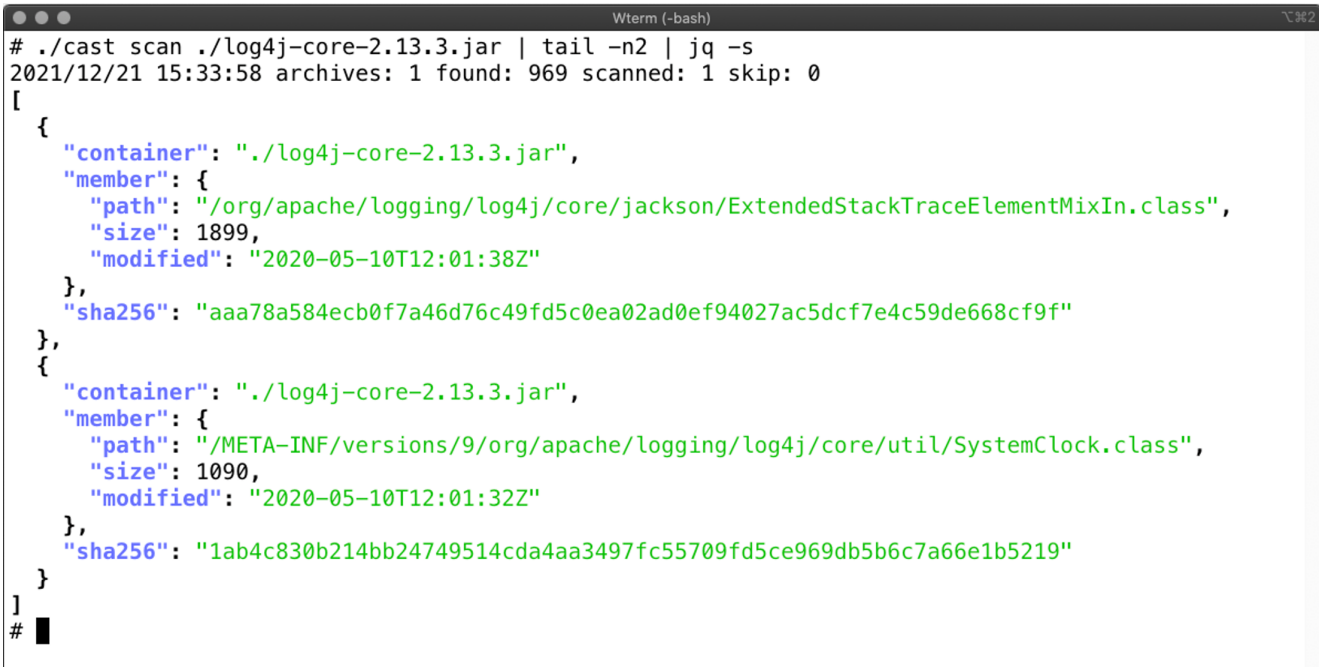
The tool is easily deployed by simply downloading the binary to your disk and then executing the binary with the directories or files you want to scan.

For example: "./cast /opt /srv /path/to/java/application"

CrowdStrike Falcon® customers also have the option to deploy and run the tool using the Falcon Real Time Response (RTR) capabilities in the Falcon sensor. A companion PowerShell script "Find-VulnerableLog4J" is included with CAST. This script is designed to be executed on Windows systems via RTR and provide actionable information to systems administrators and incident responders.

Our incident responders know that forensic triage is a continual process of ***casting*** increasingly fine nets, and identifying systems that warrant further investigation. Hence, CAST was designed to be a first-cast tool, narrowing investigative scope to a handful of machines (or paths) with known vulnerabilities.

CAST reports back in the form of a JSON file when it locates vulnerable Log4j libraries. Organizations can use this output to get an understanding of where the Log4j libraries exist across their environment so they can prioritize the systems that need to be patched using the latest security updates released by Apache.



CrowdStrike investigators use our Humio solution to load and analyze the data, but you can use any visualization solution (such as ELK). You can also work through the data with a programming language or JSON query language of your choice — the events are intended to be portable.

And finally, CrowdStrike recommends that you fully document your Log4j patching process to streamline future patch application repeatability. Since the initial discovery of the Log4j vulnerability, Apache has released three security updates (patches) at the time of this blog. Organizations that patched systems early in the process may need to reapply the latest patches, hence the need to fully document the process.

We hope you find the resources and tools in this blog useful as you cast your own net in your quest to identify Log4j vulnerabilities across your environment. We stand together when it comes to defeating adversaries that try to exploit this vulnerability against us.

One team, one fight!

Additional Resources

- *Visit the CrowdStrike Log4j Vulnerability Learning Center.*
- *Download the CrowdStrike Log4j Quick Reference Guide.*
- *Access the CrowdStrike Archive Scan Tool (CAST).*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*