Secura
A BUREAU VERITAS COMPANY

External Attack Surface Scanning

Check for Log4j Vulnerability with our Automated Tool

What is it?

External Attack Surface Scanning uses our automated tool that can find and crawl webapps, and then test the most common injection vectors for the Log4Shell vulnerability such as HTTP Headers, GET/POST requests and Cookies.

It is a broad scan, prioritizing wideness over depth. This means that not all injection vectors might be found, however, it covers all commonly scanned-for points and therefore gives a reasonable picture of the attack surface for Log4Shell. Please note that currently other potential vulnerable protocols such as SMTP are not yet included in our scanner. However we are working hard to include those also, and we will let our customers know when we have finalized it (and can re-scan existing customer's infra for better coverage).

Also important to know is that for optimal results of this scan, customers need to put our IP addresses on the allowlist of any WAF or IPS/IDS.

The scan is non-intrusive and uses the DNS requests that results from triggering the vulnerability to detect if an injection point is vulnerable. At no point is a Java class file actually downloaded and/or executed.

Verified Manually

All results are manually verified so there will be very little chance of false positives. The report will consist of the list of tested sites/IPs and the subset thereof that is vulnerable to CVE-2021-44228 and related CVEs that can be tested externally.

Deeper Testing

Deeper testing is also possible, manually going through many more injection vectors and testing potential contextual vulnerabilities (i.e. after logging into an application). This is a part of our standard **VAPT service**, be it black box, gray box, or crystal box pentesting.

Learn more?

If you have any questions, please contact us via phone or email.

+31 (0) 88 888 31 00
info@secura.com
secura.com

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
Shaping a World of Trust