of the Fortune 500 use Java

1M

attack attempts were launched in just 72 hours following the Log4Shell vulnerability disclosure

30%

of Log4Shell instances remain vulnerable

The Aftermath

Exposure

150M

Number of IaaS cloud assets and apps scanned annually

22M

Flagged 22 million vulnerable Log4j2 applications of which more than 90% were open source applications

3M

Log4Shell was detected in more than 3 million vulnerable instances

Vulnerability Trends

The vast majority of the vulnerable assets (over 80%) were on Linux

55%

A total of 16 out of Log4j2 versions were flagged, 68% of which were vulnerable versions

20%

There was a 320% spike in detections in the first year as workers returned to work

Remediation Trends

17 days

Average time to remediation after detection was 17 days

Attack Patterns

22K per week

Detected 22,000 potential attacks per week at the height of the crisis

Data Analyzed

Qualys indexed more than 10 trillion data points across its installed enterprise customer base

150B

scans and 30M

ips per year

with 75 million cloud agents deployed in hybrid IT environments globally

Qualys Research Team has released more than 70 vulnerability detections to date. We continue to update our guidance as vendors release Log4Shell patches. Please visit our Log4Shell Resource Center.

www.qualys.com/log4shell-cve-2021-44228