Log4Shell
Impact by the Numbers

90% of the Fortune 500 use Java¹

1M attack attempts were launched in just 72 hours following the Log4Shell vulnerability disclosure⁶

30% of Log4Shell instances remain vulnerable⁶

The Aftermath

1 Exposure
150M Number of Cloud Assets and Apps scanned
22M Flagged 22 million vulnerable Java applications, of which more than 60% were open source applications
3M Log4Shell was detected in more than 3 million vulnerable instances

The vulnerability was detected in more than 2,800 web applications

2 Vulnerability Trends
80% The vast majority of the vulnerable assets (over 80%) were in Linux
55% A total of 16 deinsti-Log4j2 versions were identified, of which 44% were vulnerable versions
20% There was a 220% spike in detections as the sun went down and employees returned to work

3 Threat Landscape
Nearly 68,000 vulnerabilities were found in cloud workloads

42% more than 10 trillion data points across its installed enterprise customer base

6 billion IP scans per year with 75 million cloud agents deployed in hybrid IT environments globally

55% of application installations with Log4j2 were flagged as “end of support”

The 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.

©2022 Qualys, Inc. All Rights Reserved.