LOG4J VULNERABILITIES
• IN A NUTSHELL •

What is Log4j?

Apache Log4j is a widely used Java library used in many commercial and open-source software products as a Java logging framework

Vulnerabilities

CVE-2021-44228 (RCE)
CVE-2021-45046 (RCE)
CVE-2021-45105 (DoS)

more than 28 Million

The number of times the Log4j library has been downloaded **in the past 4 months**

Make sure your...

- WAFs and IPSs block Log4j related requests
- Firewalls block outbound traffic related to Log4j
- IDS trigger alerts on Log4j related requests

Why is patching challenging?

You may encounter applications with the Log4j vulnerabilities after months

- Identifying the affected assets is hard
- External scans have limited coverage only
- Patching may not be possible for 3rd party dependencies

Log4j 2021 Timeline

Nov 24th

- Alibaba Cloud Security Team reported the Apache Log4j RCE vulnerability to Apache.

Dec 1st

- First use of the vulnerability (will be identified on Dec 10th)

Dec 10th

- Public disclosure of the first Log4j vulnerability as CVE-2021-44228.
- Picus Labs adds Log4j attack simulations to the Picus Threat Library.
- Picus Labs releases the first prevention signatures.

Dec 14th

- A new RCE vulnerability (CVE-2021-45046) found in the latest (patched) Log4j version 2.15.0
- Picus Labs adds 18 new threats that cover all known variants of Log4j attacks. Vendor signatures are also updated to the latest versions.

Dec 18th

- A new RCE vulnerability (CVE-2021-45105) found in the latest (patched) Log4j version 2.16.0

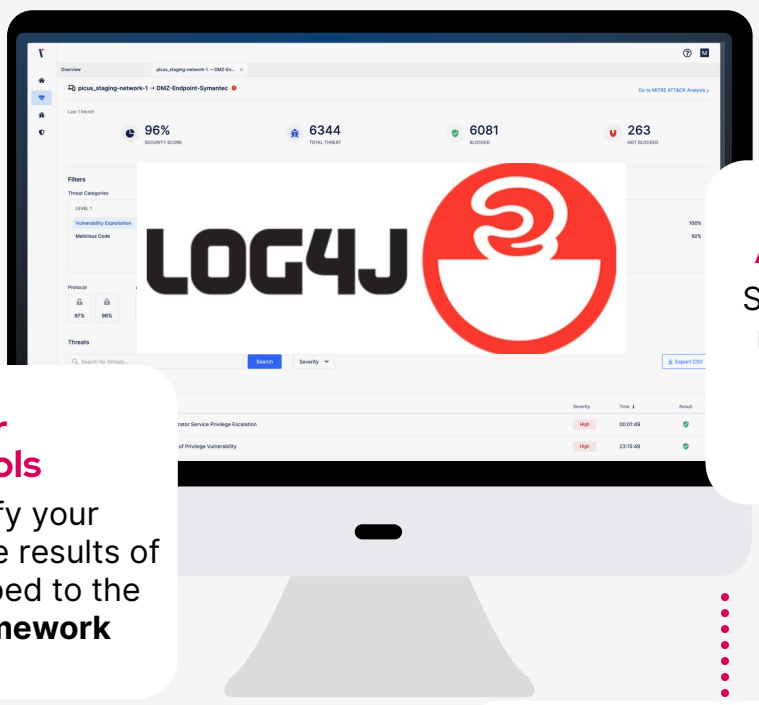
Dec 22nd

- Picus updates attacks and vendor signatures daily. Now, Picus simulates 50 different attacks and provides 93 vendor signatures for Log4j vulnerabilities.

How can you test your security controls in minutes with Picus?

Choose from a Rich Threat Library

- Picus Threat Library includes all validated threats for **Log4j vulnerabilities.** Moreover, it contains 1500+ vulnerability exploitation and endpoint attacks in addition to 11.000+ other threats as of today



Validate Your Security Controls

Automatically identify your prevention gaps. Get the results of your assessment mapped to the **MITRE ATT&CK Framework**

Run Risk-Free Attack Simulations

Safely and continuously run attack simulations against your security controls to challenge their effectiveness

Get Actionable Mitigation Signatures for Network Security Tools

- Picus Mitigation Library includes prevention signatures to address **Log4j RCE** and other vulnerability exploitation attacks

PICUS
www.picussecurity.com