WHITE PAPER

Detect log4j and other new vulnerabilities as they occur

Network detection & response solutions provide the capabilities to get out of a jam

Plixer

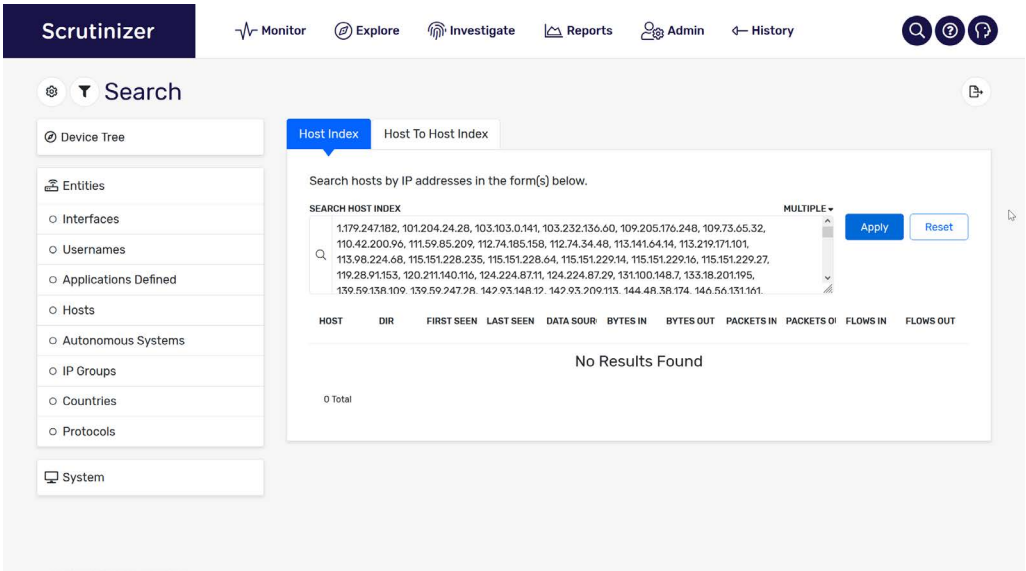
Introduction

It has happened again: a vulnerability as big as—or perhaps bigger than—the Heartbleed vulnerability (CVE-2014-0160) in OpenSSL has been discovered in a commonly used Java library called log4j. Dubbed log4jShell or log4jam (CVE-2021-44228), the vulnerability can be exploited with a specific string that allows a hacker to execute remote code, thus compromising the system.

For network and security operations teams, it is important to understand the risk to the business caused by this vulnerability, and then go about the laborious process of patching each infected system. Visibility of the network, its traffic, and the host behaviors on the network are the keys to being successful in mitigating this situation. To do this, you need a solution that can and will give a complete picture of the network. Plixer gives you that complete picture by providing pervasive visibility across the network using flow telemetry from the network infrastructure.

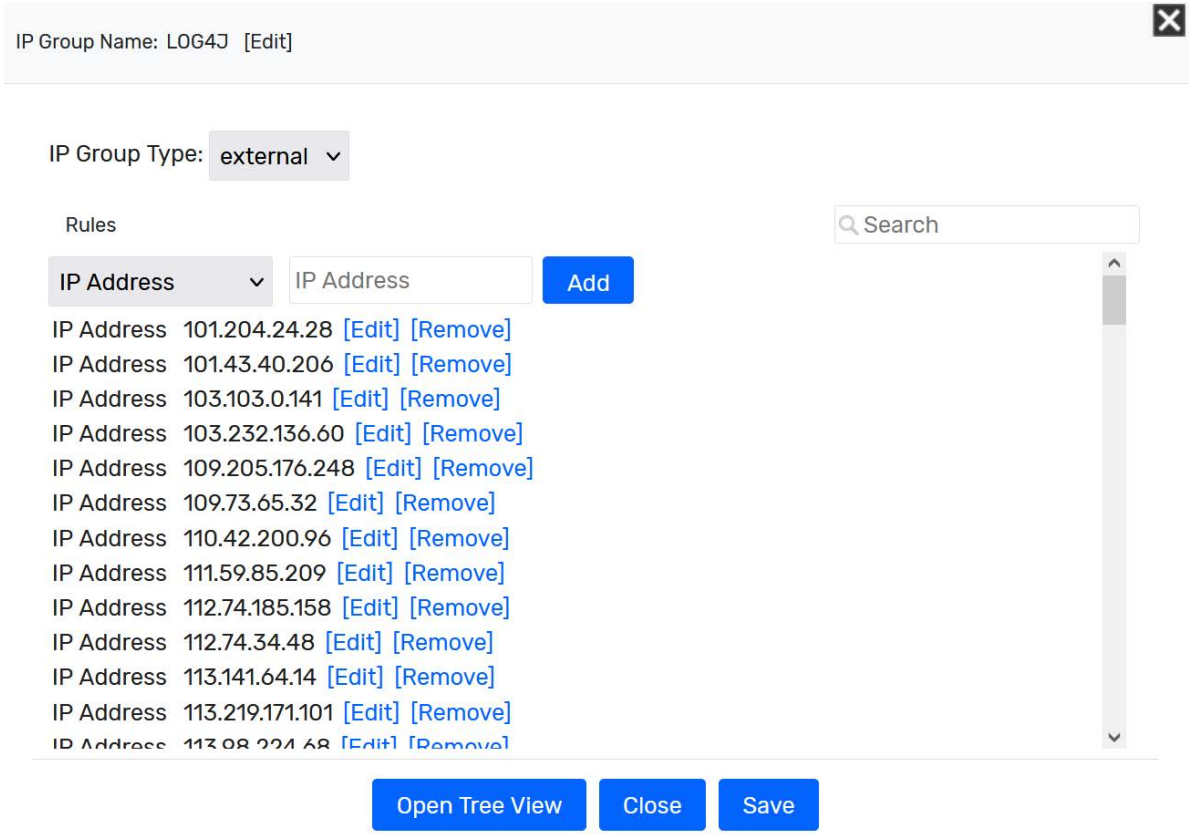
Visibility and reporting

With Plixer, security operations teams can easily determine if hosts on the network have been communicating with any of the known log4j sites. One way of doing this is to download a list of known log4j site IPs and use the host index search to filter through the metadata history. This method lets you quickly see related traffic and identify compromised hosts.

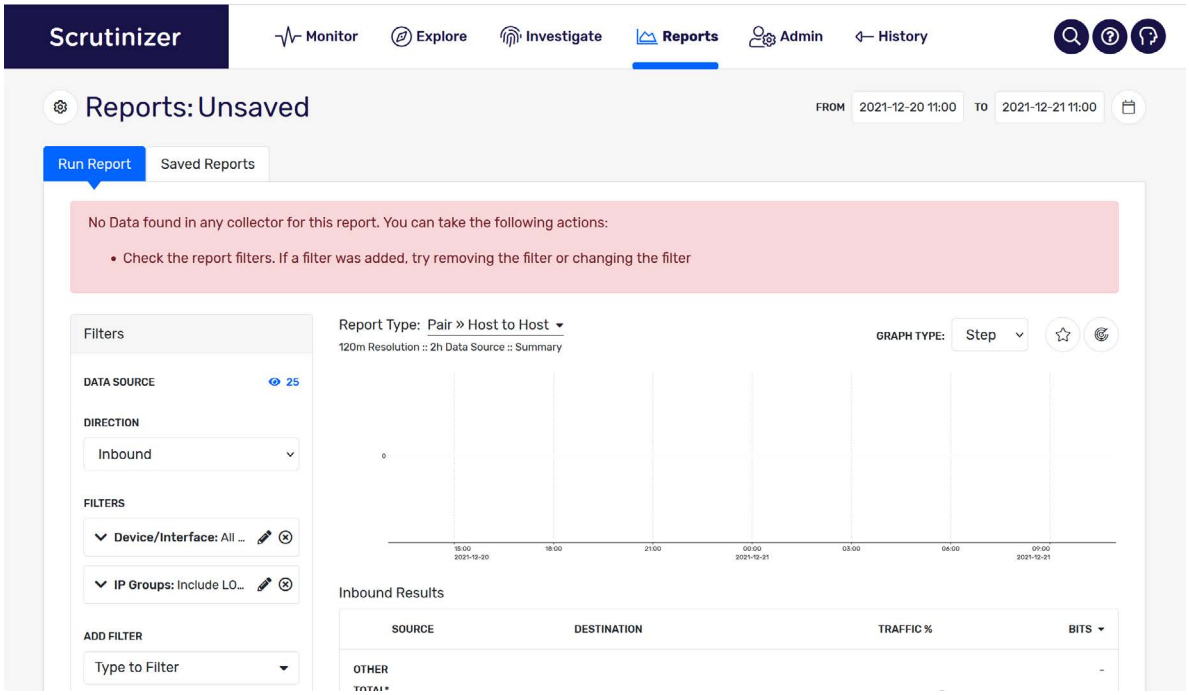


Here you can see where we copied the known list of IP's in the Host Index search function

By using this method, you get a valuable snapshot of the traffic on the network; however, the process is still manual and must be repeated regularly. A more permanent solution is to load the list of IP addresses into an IP Group. By using this IP Group as a filter with your traffic report, you can reduce multiple steps. Saving the report and adding a threshold can also automatically alert users to suspected log4j network traffic when it occurs. This report also provides contextual data that is required during the investigation and auditing process.



To help lessen the steps for regenerating this report we recommend building an IP Group and continually adding new IP's. By using this method you only need to filter by the IP Group you created.



In this example we see no traffic. This means that at the time the report was generated we are not seeing any traffic from the specified hosts.

With a few clicks of the mouse and a little configuration, Plixer can alert you when any host on the network is communicating with known log4j sites.

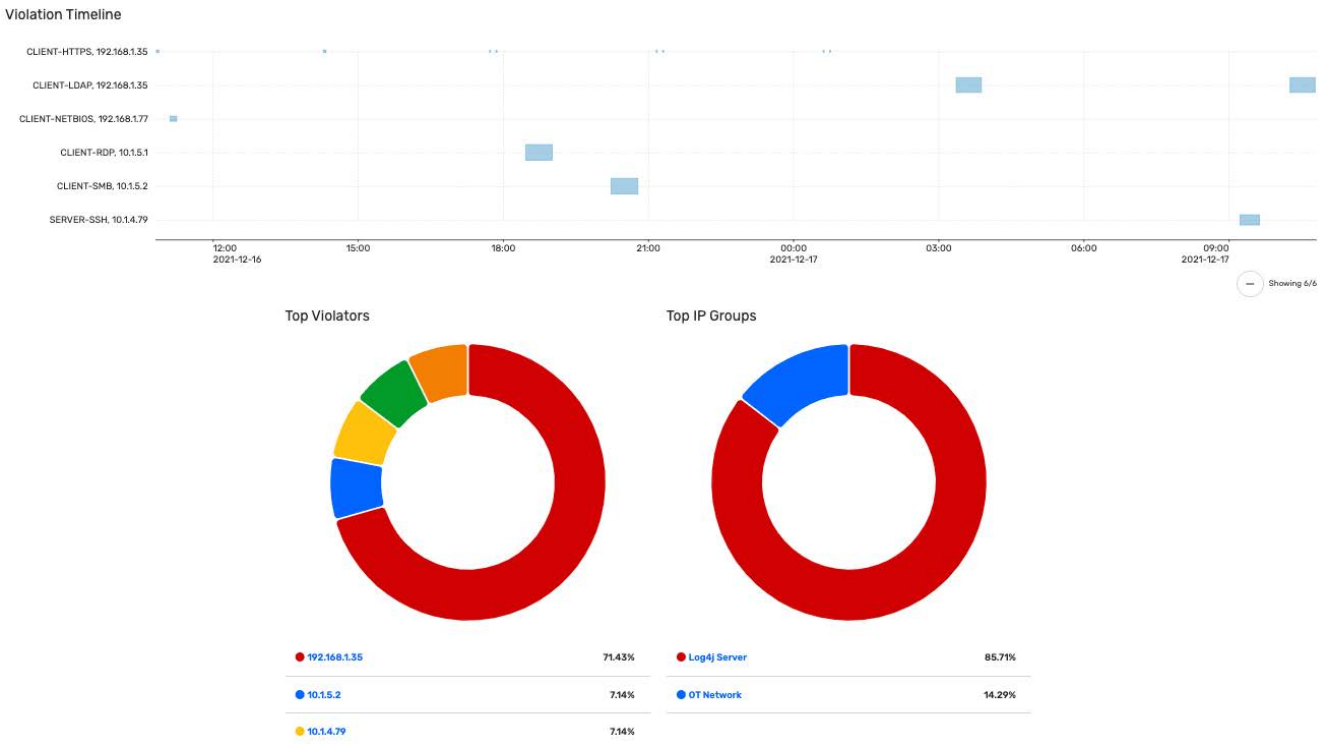
While this is a good start to protecting your network, it is still reactionary. There are improvements that we recommend, which will automate the detection of log4j malicious traffic and improve your proactive stance. The drawback to using a list of log4j sites is that these will change over time, so the configuration will have to be updated every few days manually. The next step to enhancing your approach is to employ a trusted intelligence feed via STIX/TAXII and pair it with a Network Detection and Response (NDR) solution.

Detecting the threat

Plixer's NDR platform not only provides visibility, but with advanced flow analytics and supervised/unsupervised machine learning it will detect lateral movement, indicators of compromise, data staging, and exfiltration. Log4j uses protocols like LDAP to remotely pull down malicious code and execute it on a compromised system.

Plixer's unsupervised machine learning will detect anomalous usage of key services such as LDAP, which will effectively catch log4jam during the initial compromise and lateral movement activities.

The future of log4j is uncertain at this moment. What we do know is that it will proliferate and adapt. We suggest security operations teams deploy NDR solutions like Plixer as part of a layered security strategy.

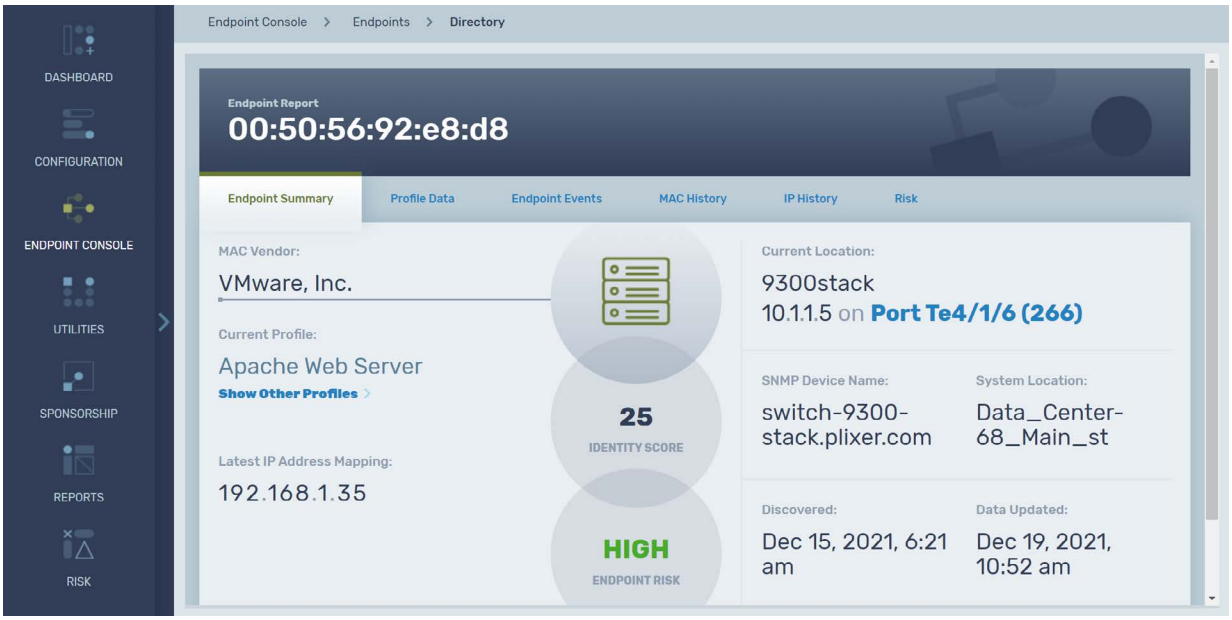


This alert is generated from Plixer's unsupervised machine learning algorithms when anomalous behaviour is detected on the LDAP service.

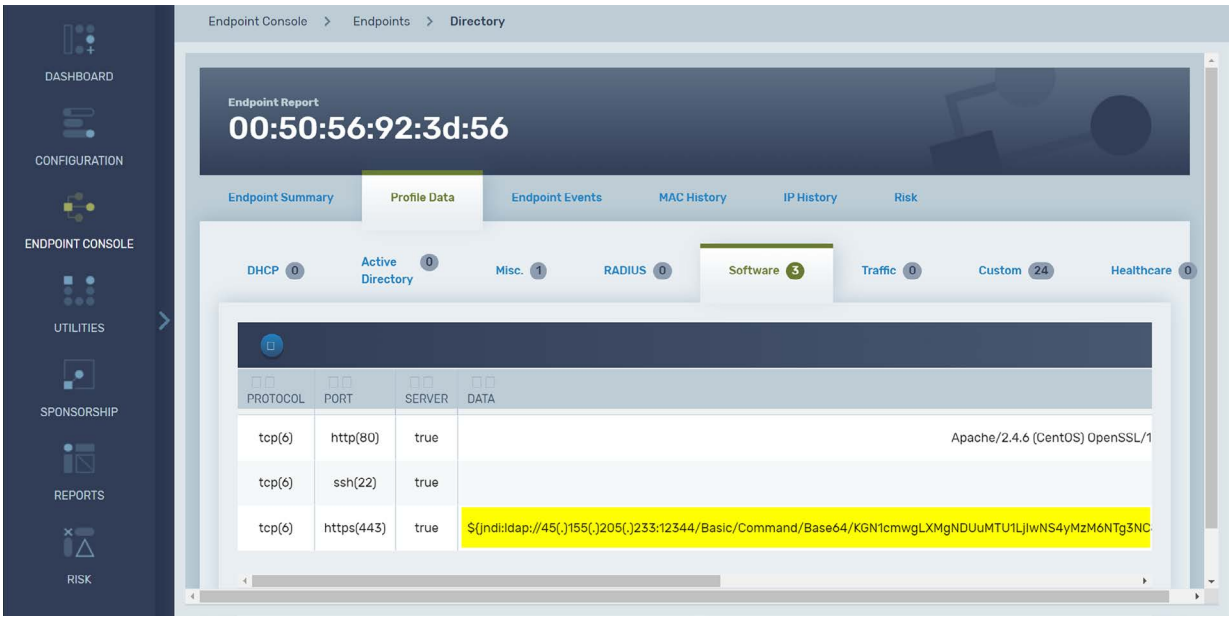
In this example, we have detected a Server-LDAP anomaly on 192.168.1.35. This means we are seeing this client send significantly more LDAP requests than are typical for this time. Furthermore, we can see that it's coming from a log4j-enabled server. This could mean something suspicious is happening.

One important feature in Plixer's NDR platform is the ability to discover and profile endpoint devices—specifically, by capturing network-based attributes and building a catalog of all network-attached hosts. One of the network-based attributes that are recorded is User-Agent strings. Using the advanced search function, any individual can search for the malicious log4j string

(${jndi:) to return a list of all compromised endpoints. Plixer's reporting engine can then help complete the picture with conversation reports, adding additional context to the hosts involved in the incident.



From the alarm we can dig into the activities of the internal host that has been communicating with the log4j IP Group. In this example we are able to see the profile of that host.



From their profile we can search endpoint data for log4j string

Plixer's NDR platform not only provides network visibility through the ingestion of flow data, but also provides a platform for early detection and device-level specifics that can help enterprises quickly respond to threats.

Conclusion

Unfortunately, log4jam won't be the last vulnerability we encounter in our lifetimes. The fact is that no matter what the vulnerability is, the steps remain the same. Detect, investigate, and report. Having a solution that gives total visibility with modern-day detection of threats is an important tool in the SecOps toolbox. Plixer's solution is the most cost-effective and versatile solution that can be shared effectively between NetOps and SecOps.

To learn more about the Plixer solution, request a demo.

About Plixer

Plixer's Network Detection and Response platform provides the intelligence and visibility needed to quickly respond to malicious network traffic. Plixer identifies anomalous behavior and provides the historical data needed to investigate threats faster. Once a threat is identified, Plixer empowers enterprises to address those threats within their existing workflow processes.