How Check Point Infinity Protects Customers from the Log4j Vulnerability

On December 9th, an acute remote code execution (RCE) vulnerability was reported in the Apache logging package Log4j 2 versions 2.14.1 and below (CVE-2021-44228). Apache Log4j is the most popular java logging library with over 400,000 downloads from its GitHub project. The Log4j library is embedded in almost every Internet service or application we are familiar with, including Twitter, Amazon, Microsoft, Minecraft and more.

Exploiting this vulnerability is simple and allows threat actors to control java-based web servers and launch remote code execution attacks.

Check Point Customers Remain Protected: Check Point has already released a new Quantum Gateway protection to prevent this attack, powered by ThreatCloud. If your Quantum gateways are updated with automatic new protections, you are already protected. Otherwise, you need to implement a new protection by following the guidelines here. We urge IT and Security teams to take immediate remediation measures on the matter.

How to ensure you are protected from the Log4j Vulnerability

1. Make sure your IPS blade is in prevention mode
2. Make sure your AppSec is in prevention mode
3. Make sure Infinity NDR is configured to detect exploited servers and internal scans on your network
4. Check your EDR for Log4j relevant incidents
5. Make sure you scan your code using SourceGuard

1. **Make sure your IPS blade is in prevention mode**

In case your setup is not configured to auto-update, you need to make sure that you are protected.

   1. Check if your gateway already contains the IPS update with the protection against the CVE through the following steps:
      a. In SmartConsole, click **Gateways & Servers**
      b. Switch the columns view to **Threat Prevention**.
      c. You will see a column with the title ‘**Installed IPS version**’ for each gateway.
      d. Make sure that all the gateways are updated with the latest package (from 12/12/2021)
e. You can also make sure that the specific protection has been updated by clicking Security Policies > Threat Prevention > IPS protections, then search for "Apache Log4j Remote Code Execution (CVE-2021-44228)"

f. Your profile column should be on prevent.
2. If you can’t see the relevant package, you need to update your setup with the latest package, by following these steps:
   a. In SmartConsole, click **Security Policies > Threat Prevention**.
   b. In the Custom Policy Tools section, click **Updates**, and then click the IPS section > **Update Now**.
   c. Install the Threat Prevention Policy.

3. Repeat step #1 to make sure you have updated all the GWs.

2. **Make sure your AppSec is in prevention mode**
   1. In the Infinity Policy dashboard, click **Cloud > Assets**.
2. Search for Log4J (CVE-2021-44228) (you can use the search bar)
3. Click on the Asset > Threat Prevention
4. Make sure that the mode is configure to Prevent.

Upgrade Apache Log4j to the latest version (2.15.0) or apply the recommended mitigations that were published by Apache on their website:
https://logging.apache.org/log4j/2.x/security.html
3. Make sure Infinity NDR is configured to detect exploited servers and internal scans on your network

4. Check your EDR for Log4j relevant incidents

5. Make sure you scan your code using SourceGuard
   1. From the Check Point Infinity Portal, download and install SourceGuard CLI according to your OS.
   2. Generate an authentication token
   3. From the command line, run: “sourceguard-cli --src <project_path>”
   4. Review the scan results in Infinity Portal to make sure you use the safe version of the Log4j library

What is ThreatCloud

You can think of ThreatCloud as a brain, and like the human brain, it is made of two lobes that work together. The right lobe, the threat intelligence, consists of millions of IoCs and telemetry updated in real time, in addition to exclusive intelligence discovered by Check Point Research, an elite group of world-renowned researchers. The left lobe, the intellect, consists of AI technology that combines the big data threat intelligence with advanced AI capabilities to detect and block never seen before threats.
Instant protections from the most significant unknown software vulnerabilities

All software vulnerabilities that are found by CPR or seen in the wild, such as Log4j, are immediately fed to ThreatCloud, which propagates the appropriate protections throughout Check Point’s products, so that all Check Point customers are instantly protected with no patching needed.

That is exactly what happened last weekend. As soon as the Log4j vulnerability was reported on December 9, all relevant protections were propagated through all of Check Point products (refer to sk176884).