Check Point
SOFTWARE TECHNOLOGIES LTD

Log4J Vulnerabilities - CheckPoint Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://blog.checkpoint.com/2021/12/11/protecting-against-cve-2021-44228-apache-log4j2-versions-2-14-1/
and https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176865.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

High

- **Response to Log4j**

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. It is used by a vast number of companies worldwide, enabling logging in a wide set of popular applications.

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

- **Affected CheckPoint Products**

There is no Check Point product to infect by these vulnerabilities.

- **CheckPoint Protection**

Check Point Software released the IPS Signature to against the Apache Log4j Remote Code Execution (CVE-2021-44228) vulnerability. We urge all customers to make sure the protection is set on prevent, to avoid the exploitation of their assets.

To find out if your setup already contains the IPS update to mitigate this vulnerability:

1. In the Gateways & Servers tab, switch the columns to Threat Prevention.
2. A column with the title installed IPS version for each gateway is shown.
3. If the version in the column is 634218276 or 635218276 or higher it includes the update.