kaspersky

卡巴斯基

CVE-2021-44228 log4j2

遠端代碼執行漏洞說明

及解決方案

卡巴斯基：關於 CVE-2021-44228 log4j2 遠端代碼執行漏洞說明及解決方案

摘要

漏洞編號：CVE-2021-44228，名稱為 Log4Shell 或者 LogJam

漏洞類型：Remote Code Execution (RCE)

組件名稱：Apache log4j2

影響範圍：2.0.0 ≦ Apache Log4j2 ≦ 2.15.0-rc1

利用難度：容易

威脅等級：嚴重

卡巴斯基檢測結果：UMIDS:Intrusion.Generic.CVE-2021-44228.*

背景描述

在 2021 年 12 月 9 日，一個 Apache log4j2 元件的嚴重遠端代碼執行漏洞被公開。Log4j Java 庫被用於 Apache 軟體基金會發佈的產品，如 Apache Struts、Apache Flink、Apache Tomcat、Apache Flume、Apache Solr、Apache Kafka 等，以及其他開源項目，如 Redis，ElasticSearch，Elastic Logstash 等。許多大型軟體公司和線上服務都使用 Log4j 庫，包括亞馬遜、蘋果 iCloud、思科、Cloudflare、ElasticSearch、Red Hat、Steam、特斯拉、Twitter 等等。與其他眾所周知的漏洞如 Heartbleed 和 Shellshock 一樣，由於其易於使用，攻擊者可以利用該漏洞遠端執行代碼，最終獲取伺服器最高許可權，目前卡巴斯基已經發現大批量在野利用。

影響範圍

Apache Log4j2 是一款非常優秀且流行的開源 Java 日誌記錄元件，在專案開發中有著廣泛的應用，其中包括企業應用程式以及大量的雲服務等。該漏洞危害性高，涉及行業和客戶廣泛，導致該漏洞潛在影響巨大。由於 Log4j2 如此受歡迎，一些資訊安全研究人員預計，未來幾天對漏洞伺服器的攻擊將顯著增加。

目前受影響的 Apache Log4j2 版本：2.0.0 ≦ Apache Log4j ≦ 2.15.0-rc1

解決方案

1. 目前，Apache 軟體基金會已發佈最新版本，建議受影響的用戶及時更新升級到最新版本 log4j-2.15.0-rc2：
   https://logging.apache.org/log4j/2.x/security.html
   https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2
2. 對於該漏洞還有一個臨時的緩解措施--設置
   log4j2.formatMsgNoLookups=true
3. 目前，卡巴斯基網路安全產品，例如 KIS（卡巴斯基安全軟體），KESL（卡巴斯基網路安全解決方案 - Linux），KES（卡巴斯基網路安全解決方案）等諸多產品都能夠成功檢測該漏洞利用，檢測結果：UMIDS:Intrusion.Generic.CVE-2021-44228.*。請確保您使用的卡巴斯基網路安全產品正確安裝並啟用各項防護元件，同時請及時更新特徵庫。

更多內容請參考如下：
https://www.kaspersky.com/blog/log4shell-critical-vulnerability-in-apache-log4j/43124/