張貼日期：2023/07/19

【漏洞預警】Juniper 產品 Junos OS 系列中的J-Web存在安全性弱點，建議請管理者儘速評估更新！

- 主旨說明：Juniper 產品 Junos OS 系列中的J-Web存在安全性弱點，建議請管理者儘速評估更新！
- 內容說明：
  - 轉發 中華資安國際 CHTSECURITY-200-202307-00000001：
  - Juniper 近日發布更新，以解決 Junos OS J-Web 所附帶的PHP軟體安全性弱點。
    - CVE-2022-31629：在 7.4.31、8.0.24 和 8.1.11 之前的 PHP 版本中，該弱點使攻擊者能夠在受害者的瀏覽器中設置不安全的 cookie：該 cookie 可被視為 “ Host-“或 ” Secure-“藉此通過 PHP 應用程式。
    - CVE-2022-31628：在 7.4.31、8.0.24 和 8.1.11 之前的 PHP 版本中：phar 解壓縮器程式碼會遞迴解壓縮”quines”gzip 的檔案，從而導致無限循環。
    - CVE-2022-31627：在 8.1.8 以下的 PHP 8.1.x 版本中，當 fileinfo 函數（例如 finfo_buffer：由於 libmagic 中的第三方程式碼使用了不正確的更新檔時，可能會使用不正確的函數來釋放分配的記憶體，這可能會導致記憶體損毀。
    - CVE-2022-31626：在7.4.30以下的PHP 7.4.x版本、8.0.20以下的8.0.x版本和8.1.7以下的8.1.x版本中，當pdo_mysql擴充帶有mysqlnd驅動程式時，如果允許第三方提供要連接的主機和連接密碼，過長的密碼可能會觸發PHP中的緩衝區溢位，從而導致遠端程式碼執行弱點。
    - CVE-2022-31625：在7.4.30以下的PHP 7.4.x版本、8.0.20以下的8.0.x版本和8.1.7以下的8.1.x版本中，當使用Postgres資料庫擴充時，參數化詢提供無效參數可能會導致PHP試圖使用未初始化的資料作為指標來釋放記憶體。 這可能導致RCE弱點或阻斷服務。
    - CVE-2021-21708：在7.4.28以下的PHP 7.4.x版本、8.0.16以下的8.0.x版本和8.1.3以下的8.1.x版本中，當使用具有filter_VALIDATE_FLOAT篩選器和最小/最大限制的篩選器函數時，如果篩選器錯誤，則有可能在閒置後觸發對已分配記憶體的使用，這可能導致記憶體損毀，並可能覆蓋其他程式碼和RCE：
    - CVE-2021-21707：在7.3.33以下的PHP版本7.3.x：7.4.26以下的7.4.x和8.0.13以下的8.0.x中，某些XML解析函數，如：simplexml_load_file：：對傳遞給它們的檔名進行URL解碼。如果該檔名包含URL編碼的NUL字元，這可能會導致函數將其解釋為檔名的末尾，從而與用戶預期的檔名解釋不同，導致其讀取與預期不同的檔案。
    - CVE-2021-21705：在7.3.29以下的PHP 7.3.x版本、7.4.21以下的7.4.x版本和8.0.8以下的8.0.x版本中，當通過帶有filter_VALIDATE_URL參數的filter_var：：函數使用URL驗證功能時，密碼欄位無效的URL可以被視為有效。 可以導致程式碼對URL錯誤解析，並可能導致其他安全隱憂，如連線錯誤的伺服器或進行錯誤的存取。
    - CVE-2021-21704：在7.3.29以下的PHP版本7.3.x：7.4.21以下的7.4.x和8.0.8以下的8.0.x中，當使用Firebird PDO驅動程式擴充時，惡意資料庫伺服器可能會回傳驅動程式未正確解析的無效回應資料，從而導致各種資料庫函數（如getAttribute：：：execute：：：fetch：：等）毀損。
    - CVE-2021-21703：在7.3.31及以下的PHP版本7.3.x：7.4.25以下的7.4.x和8.0.12以下的8.0.x中，當運行PHP FPM SAPI時，主FPM常駐程式以root用戶身份執行，子工作程序以較低權限執行時，子程序可以存取與主行程共享的記憶體並對其進行寫入，會導致root行程進行無效記憶體讀寫的方式對其進行修改，這可用於將許可權從無權限用戶提權到root用戶。
    - CVE-2021-21702：在7.3.27以下的PHP 7.3.x版本、7.4.15以下的7.4.x版本和8.0.2以下的8.0.x版本中，當使用SOAP擴充連接到SOAP伺服器時，惡意的SOAP伺服器可能會回傳格式錯誤的XML資料作為回應，影響PHP存取空指標，從而導致毀損。

        - CVE-2020-7071□在7.3.26以下的PHP 7.3.x版本、7.4.14以下的7.4.x版本和8.0.0版本中，當使用filter_var□$URL□filter_VALIDATE_URL□等函數驗證URL時，PHP將接受密碼無效的URL作為有效URL□ 這可能導致相依的URL函數錯誤地解析URL□並產生錯誤的資料作為URL的結構。
    - HiNet SOC 建議管理者儘速評估更新，以降低受駭風險。

- 影響平台:
    - Junos OS 23.2R1 之前所有版本
- 建議措施:
    - 請依照 Juniper 官網更新至建議最新版本□ Junos OS 23.2R1(含)之後所有版本
- 參考資料:
    1. https://www.cisa.gov/news-events/alerts/2023/07/13/juniper-releases-multiple-security-updates-juno-os
    2. https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-J-Web-Multiple-Vulnerabilities-in-PHP-software?language=en_US

計算機與通訊中心
網路系統組 敬啟