

張貼日期：2021/05/03

【資安漏洞預警】教育部所屬機關所使用之資訊設備疑似存在漏洞，允許攻擊者建立任意檔案於特定路徑內，進而執行任意程式碼

- 主旨說明：【資安漏洞預警】教育部所屬機關所使用之資訊設備疑似存在漏洞，允許攻擊者建立任意檔案於特定路徑內，進而執行任意程式碼

- 內容說明：

- 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202104-1319
- 本中心接獲外部情資，發現教育部所屬機關所使用之資訊設備疑似存在漏洞，可能導致遠端攻擊者可利用漏洞對目標設備建立任意檔案至特定路徑下，進而執行任意程式碼。

- 影響平台：

- CVE-2020-2509
所有QNAP設備
- CVE-2020-36195
啟用Multimedia Console與Media Streaming Add-on應用程式之QNAP設備
- CVE-2021-28798
TS-112P[TAS-168][TAS-268]之QTS 4.3.3.1624 build 20210416以前版本
- CVE-2021-28799
啟用HBS 3 Hybrid Backup Sync應用程式之QNAP設備

- 建議措施：

- 目前QNAP官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並將設備更新至以下版本：

- QTS
 - QTS 4.5.2.1566 Build 20210202(含)以後版本
 - QTS 4.5.1.1495 Build 20201123(含)以後版本
 - QTS 4.3.6.1620 Build 20210322(含)以後版本
 - QTS 4.3.4.1632 Build 20210324(含)以後版本
 - QTS 4.3.3.1624 Build 20210416(含)以後版本
 - QTS 4.2.6 Build 20210327(含)以後版本
- QuTS hero
 - QuTS hero h4.5.1.1491 build 20201119(含)以後版本
- Media Streaming Add-on
 - QTS 4.3.6: Media Streaming add-on 430.1.8.8(含)以後版本
 - QTS 4.3.3: Media Streaming add-on 430.1.8.10(含)以後版本
- Multimedia Console
 - QTS 4.4.x and later: Multimedia Console 1.3.4(含)以後版本
- HBS 3 Hybrid Backup Sync
 - QTS 4.5.2: HBS 3 Hybrid Backup Sync 16.0.0415(含)以後版本
 - QTS 4.3.6: HBS 3 Hybrid Backup Sync 3.0.210412(含)以後版本
 - QuTS hero h4.5.1: HBS 3 Hybrid Backup Sync 16.0.0419(含)以後版本
 - QuTScloud c4.5.1~c4.5.4: HBS 3 Hybrid Backup Sync 16.0.0419(含)以後版本

- 參考資料：

- <https://wwwqnap.com/en/security-advisory/qsa-21-05>
- <https://wwwqnap.com/en/security-advisory/qsa-21-11>

3. <https://wwwqnap.com/en/security-advisory/qsa-21-13>
4. <https://www.ithome.com.tw/news/144004>
5. <https://nvd.nist.gov/vuln/detail/CVE-2020-36195>
6. https://www.qnap.com/zh-tw/product_x_down/firmware_log.php
7. <https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1154>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20210503_01 

Last update: **2021/05/03 11:00**