

張貼日期：2018/05/28

[資安漏洞預警通知] 多款DrayTek路由設備存在零時差漏洞，允許攻擊者竄改DNS位址及DHCP設定，請儘速確認並進行更新！

主旨：[[資安漏洞預警通知] 多款DrayTek路由設備存在零時差漏洞，允許攻擊者竄改DNS位址及DHCP設定，請儘速確認並進行更新！

- 內容說明：

- 研究人員發現多款DrayTek路由設備存在零時差漏洞，允許攻擊者藉由攔截管理者SESSION連線，並透過遠端管理功能竄改路由設備的DNS及DHCP設定。目前已知受害設備的DNS伺服器位址會被設為38.134.121.95，導致攻擊者可將受害者瀏覽的網站轉導到惡意網站，或是竊取使用的憑證等。

- 影響平臺：

- Vigor2120 version 3.8.8.2(不含)以前版本
- Vigor2133 version 3.8.8.2(不含)以前版本
- Vigor2760D version 3.8.8.2(不含)以前版本
- Vigor2762 version 3.8.8.2(不含)以前版本
- Vigor2832 version 3.8.8.2(不含)以前版本
- Vigor2860 version 3.8.8(不含)以前版本
- Vigor2862 version 3.8.8.2(不含)以前版本
- Vigor2862B version 3.8.8.2(不含)以前版本
- Vigor2912 version 3.8.8.2(不含)以前版本
- Vigor2925 version 3.8.8.2(不含)以前版本
- Vigor2926 version 3.8.8.2(不含)以前版本
- Vigor2952 version 3.8.8.2(不含)以前版本
- Vigor3200 version 3.8.8.2(不含)以前版本
- Vigor3220 version 3.8.8.2(不含)以前版本
- VigorBX2000 version 3.8.1.9(不含)以前版本
- Vigor2830nv2 version 3.8.8.2(不含)以前版本
- Vigor2830 version 3.8.8.2(不含)以前版本
- Vigor2850 version 3.8.8.2(不含)以前版本
- Vigor2920 version 3.8.8.2(不含)以前版本

- 建議措施：

1. 進行韌體更新，步驟如下：

1. 請至官方網站下載韌體更新工具，連結如

下：<https://www.draytek.com/zh/download/software/firmware-upgrade-utility/>

2. 請至下列連結，並依照設備型號下載韌體更新檔案：<http://www.draytek.com.tw/ftp/>

3. 開啟更新工具，並填入設備IP及韌體更新檔路徑後，點選「送出」進行更新。

2. 依官網指示關閉遠端管理功能，如有需要請改用VPN進行遠端存取，方法連結如

下：<https://www.draytek.com/zh/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers>

- 參考資料：

1. <https://www.draytek.com/zh/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers>
2. <https://www.draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers>

3. <https://www.ithome.com.tw/news/123293>
4. <https://www.securityweek.com/attackers-change-dns-settings-draytek-routers>

計算機與通訊中心
網路系統組 敬啟

From:

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

Permanent link:

http://net.nthu.edu.tw/netsys/mailling:announcement:20180528_02

Last update: **2018/05/28 14:05**

