臺南一中資訊組 <mis@gm.tnfsh.tn.edu.tw>

FW: 【漏洞預警】D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)，請儘速確認並進行修補！

1 封郵件

gz710@mail.ncku.edu.tw <gz710@mail.ncku.edu.tw> 2024年4月16日 上午8:07
收件者: nckucc_黃國展 <gz710@mail.ncku.edu.tw>
副本: nckucc_朱敏清 <kkinglord@mail.ncku.edu.tw>

各位老師好：

轉寄教育機構ANA通報平台通知，謝謝。

成大 計網中心 敬上

連絡電話 : 06-2757575轉61037

From: service <service@cert.tanet.edu.tw>
Sent: Monday, April 15, 2024 4:55 PM
To: service@cert.tanet.edu.tw
Subject: (ANA事件單通知:TACERT-ANA-2024041504040303)(【漏洞預警】D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)，請儘速確認並進行修補！)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2024041504040303	發佈時間	2024-04-15 16:41:05
事故類型	ANA-漏洞預警	發現時間	2024-04-15 16:41:05
影響等級	中		

[主旨說明:]【漏洞預警】D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)，請儘速確認並進行修補！

[內容說明:]

轉發 國家資安資訊分享與分析中心 NISAC-200-202404-00000053

研究人員發現部分舊款D-Link NAS存在使用Hard-coded帳號通行碼漏洞(Use of Hard-Coded Credentials)(CVE-2024-3272)與作業系統指令注入漏洞(OS Command Injection)(CVE-2024-3273)，未經身分鑑別之遠端攻擊者可利用CVE-2024-3272提升至系統權限，或利用CVE-2024-3273執行任意程式碼。受影響之型號皆已停止支援，請儘速確認並進行汰換。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

- DNS-320L
- DNS-325
- DNS-327L
- DNS-340L

[建議措施:]

官方已宣布不再支援更新受影響之型號，請儘速確認並進行汰換

[參考資料:]
1. https://nvd.nist.gov/vuln/detail/CVE-2024-3272
2. https://nvd.nist.gov/vuln/detail/CVE-2024-3273
3. https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw