

## 政府網際服務網通報

發佈編號：GSN\_SEC\_240207

發佈日期：2024/02/07

統計期間：2024/1/1~2024/1/31

### 政府網際服務網通報摘要：

1. 本期由閘口 IPS 阻擋「重大」及「嚴重」紀錄事件統計中，共攔截 300,027,682 次次攻擊。其中依前十大惡意攻擊次數排名顯示，排名第 1 之攻擊事件為 Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass 事件攻擊數達 191,360,487 次，Netcore/Netis 網路路由設備，韌體內藏後門程式，允許攻擊者遠端執行命令、讀檔以及變更設定組態。
2. 排名第 2 之攻擊事件 AnyDesk  
事件攻擊數達 53,890,761 次，此行為特徵為 AnyDesk 應用服務，AnyDesk 為一跨平台圖形介面之遠端桌面軟體。因其可跨越防火牆之特性，攻擊者可藉由 AnyDesk 上檔案之傳輸、軟體漏洞等竊取使用者敏感資訊或取得終端主控權，以利攻擊者進一步攻擊。
3. 排名第 3 之攻擊事件為 BitTorrent  
事件攻擊數達 22,958,980 次，此行為特徵為 BitTorrent 應用服務，BitTorrent 是一種廣用的 P2P 檔案分享協定，P2P 網路可能藉由用戶間點對點檔案之傳送，造成惡意檔案或病毒由此路徑傳送，盡而促成各種網路攻擊。
4. 排名第 4 之攻擊事件 TeamViewer  
事件攻擊數達 15,868,652 次，此行為特徵為 TeamViewer 應用服務，TeamViewer 是兩終端電腦用於遠端控制、分享桌面操作與檔案傳輸之服務。因其可跨越防火牆之特性，攻擊者可藉由 TeamViewer 上檔案之傳輸、軟體漏洞等竊取使用者敏感資訊或取得終端主控權，以利攻擊者進一步攻擊。

## 政府網際服務網通報

5. 排名第 5 之攻擊事件為 Realtek.SDK.UDP.Server.Command.Execution  
事件攻擊數達 6,560,052 次，此行為表示攻擊者嘗試利用 Realtek 設備中的命令執行漏洞，該漏洞是由易受攻擊的軟體處理惡意請求時發生的錯誤引起的，攻擊者可能能夠利用此漏洞在易受攻擊的系統上執行任意代碼。
6. 排名第 6 之攻擊事件為 Linux.Kernel.TCP.SACK.Panic.DoS  
攻擊者透過利用 linux kernel 處理比較小 MSS (maximum segment size) 的 TCP 封包時產生的錯誤，利用此漏洞造成網路或服務中斷的攻擊行為。
7. 排名第 7 之攻擊事件為 Web.Server.Password.File.Access  
攻擊者試圖通過 HTTP 請求連線至敏感文件，如/etc/passwd（本地用戶列表）、/etc/shadow（用戶密碼 hash 值列表）、/etc/host（主機文件）等，Linux 系統中的這些文件存儲有關註冊用戶的基本資料。對這些文件的訪問通常須受到限制，若這些資料被不正常訪問，則可能造成使用者帳號密碼被竊取進而讓攻擊者可成功駭入該主機。
8. 排名第 8 之攻擊事件為 DNS.TXT.Records.Tunneling  
DNS Tunneling 是隱蔽通道的一種，經由將其他通信協定封裝在 DNS 通信協定中傳輸，以突破企業安全機制的限制而完成非法通訊的過程。因為在網際網路的 DNS 是一個必不可少的基礎服務，防火牆和入侵檢測系統很少會過濾 DNS 流量，這就給 DNS 作為一種隱蔽通道提供了條件，從而可以利用它實現例如遠端控制，資料傳輸作業。DNS Tunneling 也經常在殭屍網路和 APT 攻擊中扮演著重要的角色。
9. 排名第 9 之攻擊事件為 Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection  
遠端攻擊者利用指令注入漏洞攻擊 Hikvision 產品的網頁伺服器，並利用此漏洞在受影響之產品上執行任意指令。

## 政府網際服務網通報

### 10. 排名第 10 之攻擊事件為 Telnet.Default.Credentials

此行為表示攻擊者嘗試使用系統預設的 telnet 帳號與密碼登入，Mirai 等惡意軟體有時會透過掃描未關閉之 telnet 連接埠，並使用這些預設之憑證登入，而造成遠端攻擊者登入系統並加以控制。

#### 防護建議：

1. 機關委外進行弱點掃描及漏洞修補服務時，建議進行此類服務前，能先向 GSN 維運小組提出申請進行開放，避免掃描結果準確性降低。
2. 機關應定期注意各作業系統或軟體是否有發佈漏洞弱點之公告，並即時修補相關弱點，或採取相對應變措施，以避免造成資安風險。
3. 資訊系統人員應監測網站或系統連線之封包數，流量或 Sessions，如有發生異常，應保持警覺監控來源 IP，並應情況適時封鎖，以避免服務遭受阻絕式服務攻擊。
4. 網頁程式撰寫時應對輸入資料欄位進行格式及特殊字元檢查及過濾，另對於檔案上傳應檢測檔案型態，大小與內容等，以避免遭受駭客竊取資訊或植入後門程式遙控主機。
5. 各機關系統管理人員，應定期檢視防火牆連線紀錄，並過濾特殊協定封包，確認無異常連線之紀錄；若須對外網路開放服務之埠號，建議採取正面表列準則且盡量以點對點原則訂定，縮小網路開放範圍。
6. 各機關應提醒使用者，盡量勿用公務電子信箱註冊網站，以降低遭受垃圾郵件攻擊之情形。
7. 各機關網路管理人員應定期審視相關網路設備是否有異常連線，並定期稽核相關登入日誌，以降低資安風險發生之機率。
8. 如用戶發現有因入侵防禦系統誤判而導致連線異常之情況，請來電告知 GSN 維運小組設定例外排除。GSN 維運小組電話：(02) 2344-2836#1204。

## 政府網際服務網通報

### GSN 開口 等級為「high」或「critical」Top 10 攻擊事件

NO	Filter Name	Severity	Hits
	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	critical	191,360,487
	AnyDesk	high	53,890,761
	BitTorrent	high	22,958,980
	TeamViewer	high	15,868,652
	Realtek.SDK.UDPServer.Command.Execution	critical	6,560,052
	Linux.Kernel.TCP.SACK.Panic.DoS	high	1,015,225
	Web.Server.Password.File.Access	high	923,733
	DNS.TXT.Records.Tunneling	critical	833,101
	Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	critical	747,677
	Telnet.Default.Credentials	high	676,796

### GSN 開口 Top 10 攻擊事件

攻擊事件類型	事件數
QUIC	282,705,849
Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	191,360,487
AnyDesk	53,890,761
NTP.Monlist.Command.DoS	36,496,233
Nmap.Script.Scanner	35,548,647
BitTorrent	22,958,980
TeamViewer	15,868,652
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner	9,427,085
Realtek.SDK.UDPServer.Command.Execution	6,560,052
TikTok	4,371,700