張貼日期：2022/12/01

【資安攻擊預警】駭客正在銷售最新Fortinet漏洞的存取方式

- 主旨說明：駭客正在銷售最新Fortinet漏洞的存取方式

- 內容說明：
  - 轉發 科學園區資安資訊分享與分析中心 SPISAC-ANA-202212-0001。
  - 安全廠商發現，稍早發現的Fortinet網路設備軟體漏洞已經有駭客公開販售存取的方法。
  - 10月間Fortinet修補了零時差漏洞CVE-2022-40684。它是HTTP/HTTPS管理介面的驗證繞過漏洞，可被遠端濫用，風險值列為9.6，屬於重大風險。這項漏洞影響多項產品，包括FortiOS、FortiProxy和FortiSwitchManager。
  - Cyble發現的是「多個」未授權FortiOS裝置的存取資訊，包括網址、管理員用戶的SSH Key。分析這些存取資訊顯示，攻擊者企圖將公開金鑰加入到受害企業管理員帳號中，藉此冒充管理員存取Fortinet設備。根據資料，這些受害企業用的都是過時版本的FortiOS。研究人員相信，張貼廣告的攻擊者應該是對CVE-2022-40684發動攻擊。
- 影響平台：Fortinet網路設備
- 建議措施：研究人員呼籲用戶儘速安裝修補程式，因為網路上已公開的概念驗證（PoC）程式及自動化工具，讓攻擊者在漏洞公布幾天之內就能發動攻擊。
- 參考資料：
  1. https://www.ithome.com.tw/news/154488
  2. https://blog.cyble.com/2022/11/24/multiple-organisations-compromised-by-critical-authentication-bypass-vulnerability-in-fortinet-products-cve-2022-40684/
  3. https://nvd.nist.gov/vuln/detail/CVE-2022-40684/

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:20221201_04

Last update: **2022/12/01 15:02**