力麗科技
LeaLea Technology

Fortinet 安全漏洞版本更新通報

Fortinet：關於 FortiOS 存在一個使用替代路徑或通道進行身份驗證繞過漏洞 (CWE-288)，可能允許未經身份驗證的（FortiOS v7.0）遠端攻擊者透過向 Node.js WebSocket 模組發送特別設計的請求，可獲得超級管理員權限。

Fortinet：關於 FG-IR-24-535/CVE-2024-55591，建議在升級到最新版本之前立即採取措施緩解此漏洞。

解決方案，請更新至建議版本修補相關漏洞：

影響範圍:

版本	受影響的	建議版本
FortiOS	7.0.0 到 7.0.16之間版本	升級到 7.0.17 或以上
FortiProxy 7.0	7.0.0 到 7.0.19之間版本	升級到 7.0.20 或以上
FortiProxy 7.2	7.2.0 到7.2.12 之間版本	升級到 7.2.13或以上

WorkAround

- 在面對網際網路的介面上，關閉管理員存取。
- 透過Local-in Policy 限制可存取防火牆的來源IP 白名單。

入侵指標 (IoCs)

在記錄中，尋找包含 action="Add" 或 action="Edit" 的操作，會具有 ui="jsconsole" 和 method="jsconsole"，而其中 srcip 參數若與 Admin login (action="login") 的 srcip 不同，通常屬於不合法的情況。在已報告的案例中，我們觀察到的不合法 srcip 包括：

1.1.1.1

2.2.2.2

127.0.0.1

8.8.8.8

8.8.4.4

我們觀察到的案例中，威脅行為者（Threat Actor, TA）執行的操作包括以下部分或全部：

- 在設備上新增隨機用戶名的管理員帳戶
- 在設備上新增隨機用戶名的本地用戶帳戶
- 新增用戶群組，或將上述本地用戶添加到現有的 SSL VPN 用戶群組
- 添加或更改其他設定（如防火牆規則、防火牆位址等）
- 使用上述新增的本地用戶帳戶登入 SSL VPN，從而獲得通往內部網路的通道。

公開發布訊息網址

敬請注意更新訊息將不定時發佈於此網址，本文件不會再續行更新，請上此網頁取得最新資訊。

https://www.fortiguard.com/psirt/FG-IR-24-535

目前台灣地區尚未接獲因上述漏洞遭到積極利用通報，但建議未進行更新修補的 Fortinet 設備必須迅速安裝更新，以免造成網路犯罪行為者濫用。

更多詳細解決辦法請參考如下：

https://www.fortiguard.com/psirt/FG-IR-24-535