ACCELLION: FILE TRANSFER APPLIANCE (FTA) SOFTWARE

駭客是在去年的 12 月中開採了 Accellion 檔案傳輸裝置（File Transfer Appliance，FTA）軟體的零時差漏洞，Accellion 在得知後於 12 月 23 日修補了該漏洞，然而，之後 Accellion 卻發覺駭客還透過其它的 4 個 FTA 零時差漏洞，針對採用 FTA 的客戶展開攻擊，影響接近 50 家客戶。
這 4 個安全漏洞分別是 CVE-2021-27101、CVE-2021-27102、CVE-2021-27103 與 CVE-2021-27104，當中的 CVE-2021-27101 屬於 SQL 隱碼（SQL injection）漏洞，允許未經授權遠端使用者執行命令，而駭客即利用該漏洞於受害系統上部署了名為 Dewmode 的 Web Shell，以用來竊取資料。

零時差漏洞或**零日漏洞**（英語：**0**-day vulnerability、zero-day vulnerability）是指軟體、韌體或硬體設計當中已被公開揭露但廠商卻仍未修補的缺失、弱點或錯誤。或許，研究人員已經揭露這項漏洞，廠商及開發人員也已經知道這項缺失，但卻尚未正式釋出更新來修補這項漏洞。
0day(zero-day 又稱零時差漏洞)是指系統存在未即時修補的漏洞，攻擊者利用此漏洞入侵他人電腦。近年來惡意攻擊的目標，不再侷限於癱軟他人電腦及設備似惡作劇的手法，反而是在入侵受害者的系統後，隱密且持續地取得內部資料，並藉此換取金錢利益。

「**零時差**」（Zero Day）是軟體或硬體中「尚未」被修補的瑕疵。只要這個零時差漏洞尚未曝光，軟體和硬體公司自然不會去修復它（因為他們根本還不知道有這漏洞），網路攻擊就能持續進行。這種攻擊包含了資料竊取、資料監聽、檔案銷毀…等，

SQL 注入（英語：SQL injection），也稱 **SQL 隱碼**或 **SQL 注碼**，是發生於應用程式與資料庫層的安全漏洞。簡而言之，是在輸入的字串之中夾帶 SQL 指令，在設計不良的程式當中忽略了字元檢查，那麼這些夾帶進去的惡意指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因此遭到破壞或是入侵。

SQL 隱碼攻擊是一種網站弱點，能讓攻擊者使用資料庫查詢語法入侵網站的資料庫， 一般都是正常查詢命令夾雜 SQL 惡意命令，在未過濾 SQL 惡意命令的情況下，資料庫伺服器會接收到攻擊代碼並執行，使得攻擊者能擅自更動、刪除、或竊取資訊。