

張貼日期：2023/12/21

【漏洞預警】OMICARD EDM行銷發送系統 v6.0.1.5存在漏洞，建議請管理者儘速評估更新！

- 主旨說明：OMICARD EDM行銷發送系統 v6.0.1.5存在漏洞，建議請管理者儘速評估更新！
- 內容說明：
 - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202312-00000004
 - OMICARD EDM行銷發送系統漏洞說明如下：
 - CVE-2023-48373 OMICARD EDM行銷發送系統 v6.0.1.5 沛盛資訊 OMICARD EDM 行銷發送系統特定頁面存在Path Traversal漏洞，未經驗證之遠端攻擊者可利用此漏洞繞過身分認證機制，讀取任意系統檔案。
 - CVE-2023-48372 OMICARD EDM行銷發送系統 v6.0.1.5 沛盛資訊 OMICARD EDM 行銷發送系統的SMS相關功能存在SQL Injection 漏洞，遠端攻擊者不須權限，遠端攻擊者不須權限，即可注入任意SQL語法讀取、修改及刪除資料庫。
 - CVE-2023-48371 OMICARD EDM行銷發送系統 v6.0.1.5 沛盛資訊 OMICARD EDM 行銷發送系統之上傳功能未對上傳檔案進行檢查限制，導致遠端攻擊者不須登入，即可以上傳任意檔案，進而執行任意程式碼或中斷系統服務。
- 影響平台：
 - 沛盛資訊 OMICARD EDM行銷發送系統 v6.0.1.5
- 建議措施：
 - 更新版本至v5.9之後之版本
- 參考資料：
 - <https://www.twcert.org.tw/tw/lp-132-1.html>

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:20231221_05

Last update: 2023/12/21 15:16