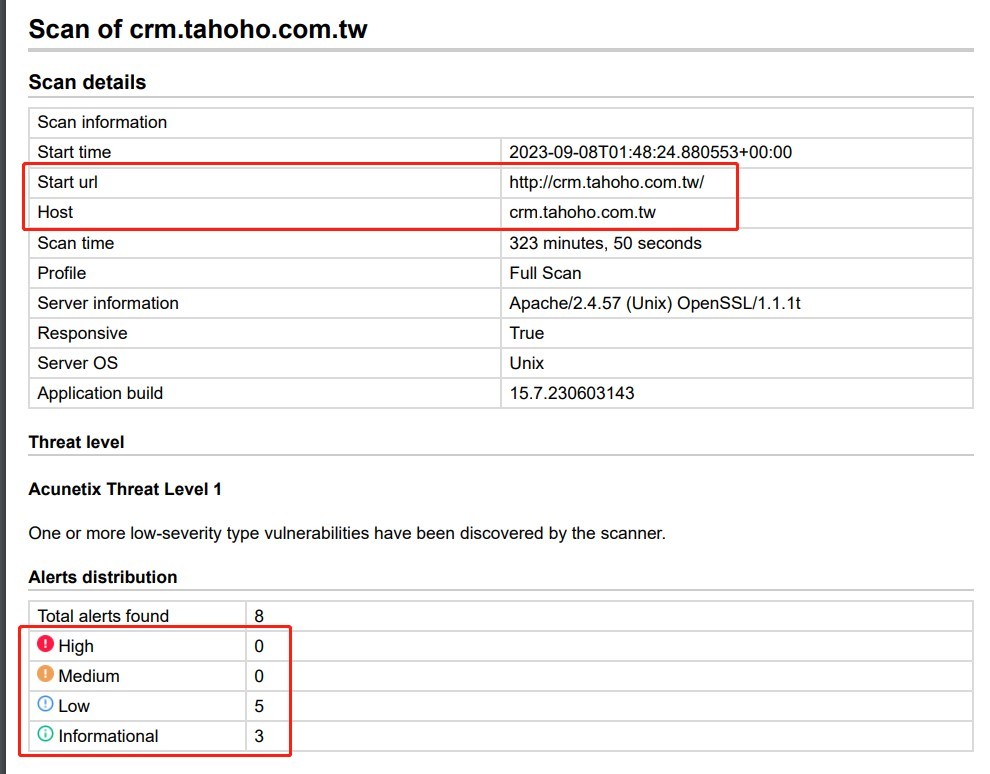
**From:** 總公司 廖毓銘 <joy.liao@tahoho.com.tw>   
**Sent:** Monday, September 11, 2023 10:08 AM  
**To:** 許心瑀 <shvon@tcci.com.tw>; 施谷澤 <Ted.shih@tcci.com.tw>  
**Cc:** 總公司 駱正達 <chengta.lo@tahoho.com.tw>; 李振銘 <Jimmy.Lee@tcci.com.tw>; 傅柏貴 <Neo.Fu@tcci.com.tw>  
**Subject:** [外部郵件]回覆: 請協助處理其CRM系統之弱點(High)

Dear Shvon:

   通報原廠後，其CRM之前所回報的SQL Injection問題，目前未被再次掃描到。謝謝



廖毓銘 /Joy Liao

IT/Information Security Manager

Onyx TaHo Environmental Services Co., Ltd.

ISC2 Taiwan Chapter Director

Tel: +886-2-2586-0177 ext 354

Mobile: 0929-160-831/ 0910653630

CISSP/CISM/PMP/ISO 27001、27701 Lead Auditor

IEC 62443-2-1 Lead Auditor

**寄件者:** 總公司 廖毓銘 <[joy.liao@tahoho.com.tw](mailto:joy.liao@tahoho.com.tw)>  
**寄件日期:** 2023年9月1日 下午 02:47  
**收件者:** [shvon@tcci.com.tw](mailto:shvon@tcci.com.tw) <[shvon@tcci.com.tw](mailto:shvon@tcci.com.tw)>; [Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw) <[Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw)>  
**副本:** 總公司 駱正達 <[chengta.lo@tahoho.com.tw](mailto:chengta.lo@tahoho.com.tw)>; [Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw) <[Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw)>; [Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw) <[Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw)>  
**主旨:** 回覆: 請協助處理其CRM系統之弱點(High)

Dear Shvon:

cid:f3840741-229f-4cbd-a541-57b92cb21477，該報告也有在之前通報時附上，來源為Veolia-China。

  \*目前所提報的程式訊息，我會再回報回原廠

另外，在程式、DB所在的主機，也有掃瞄出弱點，在責任歸屬下，是屬於貴公司嗎?

若是，請參考附件，進行修復。\*為何會安裝NotePad++?該程式，目前出現弱點。

<https://cybersecuritynews.com/multiple-notepad-flaw/?amp>

|  |  |
| --- | --- |
|  | [Multiple Notepad++ Flaws Let Attackers Execute Arbitrary Code](https://cybersecuritynews.com/multiple-notepad-flaw/?amp)  Several Buffer Overflow vulnerabilities have been discovered in Notepad++ that can be exploited by threat actors for malicious purposes.  cybersecuritynews.com |

廖毓銘 /Joy Liao

IT/Information Security Manager

Onyx TaHo Environmental Services Co., Ltd.

ISC2 Taiwan Chapter Director

Tel: +886-2-2586-0177 ext 354

Mobile: 0929-160-831/ 0910653630

CISSP/CISM/PMP/ISO 27001、27701 Lead Auditor

IEC 62443-2-1 Lead Auditor

**寄件者:** [shvon@tcci.com.tw](mailto:shvon@tcci.com.tw) <[shvon@tcci.com.tw](mailto:shvon@tcci.com.tw)>  
**寄件日期:** 2023年8月29日 上午 10:39  
**收件者:** 總公司 廖毓銘 <[joy.liao@tahoho.com.tw](mailto:joy.liao@tahoho.com.tw)>; [Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw) <[Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw)>  
**副本:** 總公司 駱正達 <[chengta.lo@tahoho.com.tw](mailto:chengta.lo@tahoho.com.tw)>; [Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw) <[Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw)>; [Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw) <[Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw)>  
**主旨:** RE: 請協助處理其CRM系統之弱點(High)

毓銘早:

這幾天我們已檢查過程式, 不太可能會有SQL Injection(程式碼片段如下截圖。)

推測問題點應該不在我們的 server 或程式，比較有可能是中間的設備

弱掃是從外網進行的，或許我們用內部或測試系統不準

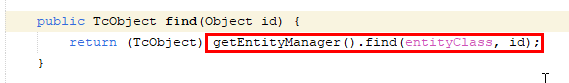
不知道貴公司掃弱是和那家廠商合作

是不是可以請該廠商和你我三方一起查明問題



tahocrm/download程式碼:





**From:** 總公司 廖毓銘 <[joy.liao@tahoho.com.tw](mailto:joy.liao@tahoho.com.tw)>   
**Sent:** Wednesday, August 23, 2023 11:01 AM  
**To:** 許心瑀 <[shvon@tcci.com.tw](mailto:shvon@tcci.com.tw)>; 施谷澤 <[Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw)>  
**Cc:** 總公司 駱正達 <[chengta.lo@tahoho.com.tw](mailto:chengta.lo@tahoho.com.tw)>; 李振銘 <[Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw)>; 傅柏貴 <[Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw)>  
**Subject:** [外部郵件]回覆: 請協助處理其CRM系統之弱點(High)

Dear Shvon:

  此為Acunetix軟體，從外部掃描後的報告。

1.Acunetix軟體本身，內部如何掃描，基本上我不會知道，但他所掃出的正確性，相信網路上資料可以查找相關資料。

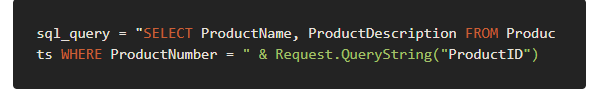
2.程式如何編寫，我也不會知道，這是你們的專業。

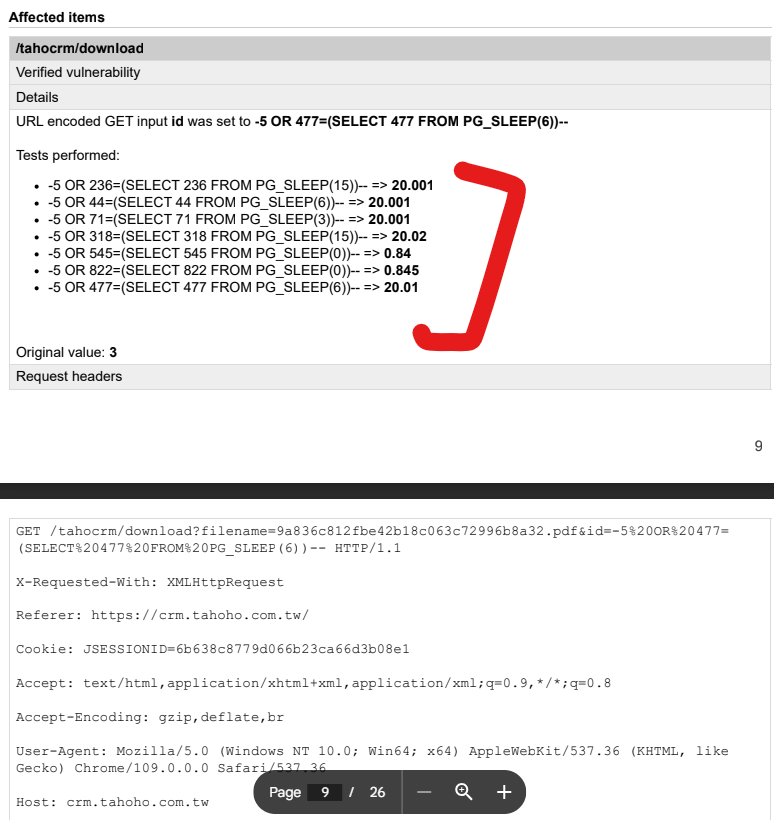
3.若照報告上的說明，查測無此問題，不是跟我堅持本身的程式無問題，可否將其輔助或測試的報告來佐證?

4.報告上的程式碼，若數字部分為程式碼使用查詢參數後，所解析出來的值，則可將其回應給原廠，請原廠確認。

    但如果是使用拼湊SQL語法方式，那就請修正。

   \*SQL Injection的攻擊手法，已經出現許多年，但近期所識別出來的問題，多為此問題，這點我比較疑惑。





廖毓銘 /Joy Liao

IT/Information Security Manager

Onyx TaHo Environmental Services Co., Ltd.

ISC2 Taiwan Chapter Director

Tel: +886-2-2586-0177 ext 354

Mobile: 0929-160-831/ 0910653630

CISSP/CISM/PMP/ISO 27001、27701 Lead Auditor

IEC 62443-2-1 Lead Auditor

**寄件者:** [shvon@tcci.com.tw](mailto:shvon@tcci.com.tw) <[shvon@tcci.com.tw](mailto:shvon@tcci.com.tw)>  
**寄件日期:** 2023年8月23日 上午 10:08  
**收件者:** 總公司 廖毓銘 <[joy.liao@tahoho.com.tw](mailto:joy.liao@tahoho.com.tw)>; [Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw) <[Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw)>  
**副本:** 總公司 駱正達 <[chengta.lo@tahoho.com.tw](mailto:chengta.lo@tahoho.com.tw)>; [Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw) <[Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw)>; [Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw) <[Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw)>  
**主旨:** RE: 請協助處理其CRM系統之弱點(High)

毓銘:

  我們在公司有自己做了檢測, 模擬不出來你的問題

 和６月底你提出發現弱點的狀況一樣

  請問你是用什麼方式或動作做的檢測

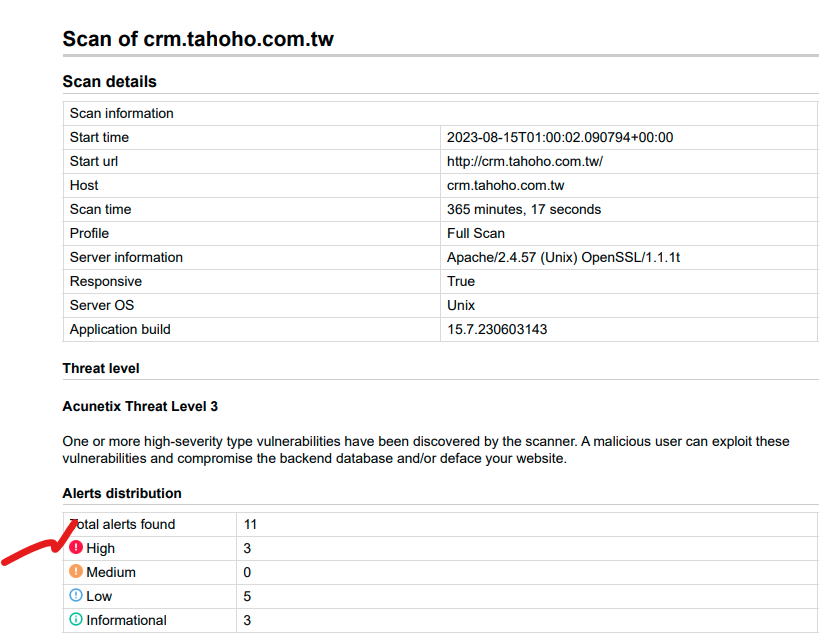
  請給我們你測試的步驟, 讓我可以產出同樣的結果找出問題

心瑀

**From:** 總公司 廖毓銘 <[joy.liao@tahoho.com.tw](mailto:joy.liao@tahoho.com.tw)>   
**Sent:** Monday, August 21, 2023 5:43 PM  
**To:** 施谷澤 <[Ted.shih@tcci.com.tw](mailto:Ted.shih@tcci.com.tw)>  
**Cc:** 總公司 駱正達 <[chengta.lo@tahoho.com.tw](mailto:chengta.lo@tahoho.com.tw)>; 李振銘 <[Jimmy.Lee@tcci.com.tw](mailto:Jimmy.Lee@tcci.com.tw)>; 許心瑀 <[shvon@tcci.com.tw](mailto:shvon@tcci.com.tw)>; 傅柏貴 <[Neo.Fu@tcci.com.tw](mailto:Neo.Fu@tcci.com.tw)>  
**Subject:** [外部郵件]請協助處理其CRM系統之弱點(High)

Dear Ted:

    敬請協助處理，其CRM系統被掃瞄出弱點，請參考附件~謝謝



廖毓銘 /Joy Liao

IT/Information Security Manager

Onyx TaHo Environmental Services Co., Ltd.

ISC2 Taiwan Chapter Director

Tel: +886-2-2586-0177 ext 354

Mobile: 0929-160-831/ 0910653630

CISSP/CISM/PMP/ISO 27001、27701 Lead Auditor

IEC 62443-2-1 Lead Auditor

|  |
| --- |
| 注意事項: 此電子郵件來自於公司外部，為了避免社交工程帶來資安危害，請再確認寄件者與主旨內容是與你工作相關，而且認知來源，否則請不要點擊連結、下載圖片、打開附件或轉發，並立即刪除。 CAUTION: This email originated from outside of organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. When in doubt or suspicion of phishing, contact your IT department immediately. |

|  |
| --- |
|  |

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

|  |
| --- |
| 注意事項: 此電子郵件來自於公司外部，為了避免社交工程帶來資安危害，請再確認寄件者與主旨內容是與你工作相關，而且認知來源，否則請不要點擊連結、下載圖片、打開附件或轉發，並立即刪除。 CAUTION: This email originated from outside of organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. When in doubt or suspicion of phishing, contact your IT department immediately. |

|  |
| --- |
|  |

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

DISCLAIMER:  
This message and any attachment may contain information that is confidential, proprietary, privileged or otherwise protected from disclosure under applicable laws. If you are not the intended recipient, you must not use, disclose, print, copy or disseminate to any person this message or any information contained in this message. If you have received this message in error, please advise the sender immediately and destroy or delete this message and any attachment from your system. THANK YOU.  
聲明:  
本訊息及其附件可能包含機密、專有、特許或依法受保護之資訊。如果您不是本訊息所載之收件人，切勿使用、揭露、列印、複製或散播本訊息或其內含資訊。若您非所載之收件人而收到本訊息，請您立刻通知送件者，並從您的系統中將本訊息及其附件銷毀或刪除。謝謝。

|  |
| --- |
| 注意事項: 此電子郵件來自於公司外部，為了避免社交工程帶來資安危害，請再確認寄件者與主旨內容是與你工作相關，而且認知來源，否則請不要點擊連結、下載圖片、打開附件或轉發，並立即刪除。 CAUTION: This email originated from outside of organization. Do not click links or open attachments unless you recognize the sender and know the content is safe. When in doubt or suspicion of phishing, contact your IT department immediately. |

|  |
| --- |
|  |