TLP:WHITE

從 Struts2 漏洞看資安事件通報

Announcement Advisory Report (ANAR)

2017-05-11

TWCERTCC-ANAR-2017005

Summary

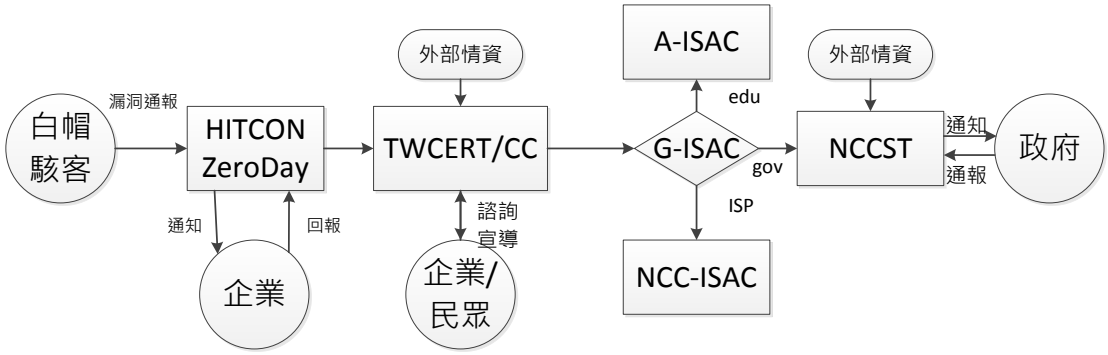
- 免費的開放原始碼網站應用程式開發框架(例如 Apache Struts2)，雖然企業可以普遍使用做為開發用途，但是無專人維護程式，漏洞可能遭駭客利用，企業仍需考慮其安全風險。
- 使用 Apache Struts2 開發之網站應盡快更新至 Apache Struts 2.3.32 或 2.5.10.1 版本。
- TWCERT/CC 除於官網及臉書粉絲專頁發布 Apache Struts2 漏點與修補方式外，更以積極的態度，結合白帽駭客與民間資安專家們的專業與力量，主動的發掘國內存在未修補 Struts2 漏洞的網站，並連繫業主進行改善。
- 當企業或民眾發生資安事件時，可向電腦安全事件應變中心尋求協助，透過情資共享能夠以先前的案例做為借鏡，防患於未然。惟目前台灣尚未有相關安全政策及法規，規範一般企業與民眾在發生資安事件時須進行通報之義務，因此後續仍需加強宣導企業及民眾的資安意識與參與度，以強化整體通報機制。

Description

Apache Struts2 是一種免費的 Java 網站應用程式開發框架，其程式碼與文件是由 Apache 軟體基金會負責維護。該框架於 2017 年初被發現負責處理檔案上傳封包的 jakarta 解析程式(Parser)存在漏洞，可讓遠端攻擊者寄送惡意封包，使攻擊者可遠端執行任意程式碼，可以導致網站資料外洩、被植入木馬程式等風險[1]，主要影響版本包含 Struts 2.3.5、Struts 2.3.31、Struts 2.5～Struts 2.5.10 版本。美國國家標準技術研究所(National Institute of Standards and Technology, NIST)的 CVSS v3 base 的評比亦顯示該漏洞為 10 的最嚴重等級[2]，表示該漏洞不但容易被駭客利用，且危害情節重大，2017 年 3 月 6 日 Apache 軟體基金會亦已發布 Struts2 的安全更新[3]。

在此漏洞遭揭露初期，TWCERT/CC 收到來自 HITCON ZeroDay 的重大漏洞通報，表示目前網路上已經有許多成功驗證(POC)S2-045 漏洞的攻擊程式，駭客可輕易的從網際網路下載攻擊程式，即可成功入侵網站伺服器，臺灣已經有使用 Struts2 框架的銀行和電信業者，遭到駭客大規模的 IP 掃描，一旦銀行業者沒有修補相關漏洞，即可能會遭受 Struts2 漏洞攻擊。TWCERT/CC 收到此通報，立即透過官方網站及臉書粉絲團公布資訊，說明此漏洞的嚴重性，並呼籲儘速修補。

HITCON ZeroDay 是由台灣駭客年會(Hacks In Taiwan, HITCON)所設立的公益性漏洞通報平台，白帽駭客與民間資安專家們可透過此平台進行善意的漏洞通報，希望藉由漏洞的精確描述(包括：詳實的文字或圖片說明、攻擊封包 Payload 等)及修復建議等，來協助企業精準地修復漏洞，也能讓企業更加注重資安問題、信賴資安專業人才。自 2016 年 1 月 1 日成立至今，TWCERT/CC 即成為 HITCON ZeroDay 之主要合作的組織，HITCON ZeroDay 成員在網際網路上所發現有關台灣地區的資安漏洞，可透過 HITCON ZeroDay 平台進行提報，經其內部初步驗證屬實後，再提供給 TWCERT/CC，TWCERT/CC 透過政府的情資分享平台(Government Information Sharing and Analysis Center, G-ISAC)再將此漏洞情資分享給其他相關領域。



如上圖所示，當 TWCERT/CC 於接獲 HITCON ZeroDay 資安專家通報資安事件與漏洞情資時，若此情資影響範圍為民間企業或民眾，TWCERT/CC 將主動向企業或民眾通知修補資訊。若情資影響範圍屬於台灣政府、學術研究單位，則透過 G-ISAC 平台分別通報給各機關，屬政府部門即通報給行政院國家資通安全會報技術服務中心(National Center for Cyber Security Technology, NCCST)、屬教育機構則通報給教育學術資訊分享與分析中心(Academy Information Sharing and Analysis Center, A-ISAC)；非屬上述情況，則向國家通訊傳播委員會資訊分享與分析中心(National Communications Commission Information Sharing and Analysis Center, NCC-ISAC)通報。

在本起 Struts 2 漏洞事件，自 2017 年 3 月 9 日起，TWCERT/CC 陸續接獲國內 HITCON 資安專家及國內外單位通報，掌握了國內 65 個單位存有 Struts2 漏洞(15 個屬政府部門、20 個屬學術研究單位、30 個屬一般民間企業)，TWCERT/CC 依循上述通報機制，透過 G-ISAC 平台分享此漏洞攻擊情資，並持續追蹤 30 個屬一般民間企業責任區內之弱點修補狀況。

TWCERT/CC 主責為中小企業與民間資安事件之通報與應變，以上案例顯示，我們正以更積極的態度，結合白帽駭客與民間資安專家們的專業與力量，主

動的發掘國內存在未修補 Struts2 漏洞的網站，並連繫業主進行改善。同時也呼籲企業或軟體廠商在使用免費開源碼或框架開發資訊系統時，應更積極地掌握到漏洞通報及修補方式，以降低企業或客戶遭駭客透過資安漏洞進行攻擊的風險。

Recommendations

1. 使用 Apache Struts2 開發之網站應盡快更新至 Apache Struts 2.3.32 或 2.5.10.1 版本。
2. 由於 Apache Struts 2 為免費的開放原始碼框架，雖然企業可以普遍使用該框架做為開發用途，但是仍需考慮其安全風險，包含開放原始碼的版本控管、許多漏洞存在許久且程式碼無專人維護不易修補等。因此程式開發人員需要經過軟體安全開發教育訓練，而對於開發完成之程式碼也須經過源碼檢測，以降低開發時造成的資安風險。企業使用開放式框架時也應考量其安全性，以免容易遭駭客入侵，影響商譽。
3. 盡可能讓作業系統、應用程式保持在官方最新的安全更新。
4. 強化完善的資安通報機制，當資訊系統存在資安風險時，能夠透過通報機制儘速掌握到漏洞原因及修補方式，以降低企業或客戶遭駭客透過資安漏洞進行攻擊的機會；當發生資安事件時，應該通報當地資通安全事件處理小組，可協助處理及排除資安風險。

References

[1] Apache, March 19, 2017, "S2-045", Retrieved May 11, 2017 from the World Wide Web: https://cwiki.apache.org/confluence/display/WW/S2-045

[2] NIST, March 10, 2017, "CVE-2017-5638 Detail", Retrieved May 11, 2017 from the World Wide Web: https://nvd.nist.gov/vuln/detail/CVE-2017-5638#vulnDescriptionTitle

[3] Github, March 6, 2017, "apache/struts", Retrieved May 11, 2017 from the World Wide Web: https://github.com/apache/struts/releases

聯繫資訊

台灣電腦網路危機處理暨協調中心

- 免付費專線：0800-885-066
- 資安事件通報 03-4115387 或 02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站: https://www.twcert.org.tw/
- Facebook: http://www.facebook.com/twcertcc