行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2017-0016	發布時間	Wed Feb 22 14:36:58 CST 2017
事件類型	漏洞預警	發現時間	Sat Feb 18 00:00:00 CST 2017
警訊名稱	NoSQL 資料庫預設配置無身分驗證機制，導致駭客可任意連線竄改資料庫內容，恐有資訊洩露或遭惡意利用之疑慮，請盡速確認並進行修正。		
內容說明	安全研究人員 Victor Gevers 於 2016/12/27 揭露針對 NoSQL 資料庫的勒索攻擊手法，由於 NoSQL 資料庫預設配置無身分驗證機制，導致駭客可任意連線竄改資料庫內容，估計全球至少 45,000 個 NoSQL 資料庫內容遭駭客刪除並勒索。 技服中心接獲外部情資發現，部分政府機關之 NoSQL 資料庫暴露於網際網路中，恐遭駭客入侵之虞，請各機關盤點與檢視是否使用相關資料庫，加強權限控管並避免使用公開的網際網路位置，以及加強防範措施。 若發現資料庫遭到入侵，請立即進行通報應變處置。		
影響平台	允許未授權外部使用者進行連線之 NoSQL 資料庫		
影響等級	低		
建議措施	1. 常見 NoSQL 資料庫包括 Redis(6379 埠口) 、CouchDB(5984 埠口)、MongoDB(27017 埠口)、Cassandra(9042 或 9160 埠口)及 ElasticSearch(9200 埠口)，請機關進行內部盤點與檢視是否使用相關 NoSQL 資料庫。 2. 定期備份資料庫資料 3. 資料庫建立權限控管機制，不允許非授權之使用者進行資料存取。 4. 資料庫所有帳號設定強健的密碼，非必要使用的帳號請將其刪除或停用。 5. 建議資料庫不要使用公開的網際網路位置，如無法避免使用公開的網際網路位置，建議資料庫前端需有防火牆防護，並採用白名單方式進行存取過濾。		

	6. 檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠。 7. 若無防火牆可考慮安裝防火牆或於 Windows 平台使用 Windows XP/7/8/2008 內建之 Internet Firewall/Windows Firewall 或 Windows 2000 之 TCP/IP 篩選功能。Linux 平台可考慮使用 iptables 等內建防火牆。 8. 建議將資料庫更新至最新版本
參考資料	1. The Ransomware Problem: Database Security in 2017 (https://www.hurricanelabs.com/blog/ransomware-problem-database-security-2017) 2. MongoDB Databases Held for Ransom by Mysterious Attacker(https://www.bleepingcomputer.com/news/security/mongodb-databases-held-for-ransom-by-mysterious-attacker/) 3. MongoDB Manual-Security(https://docs.mongodb.com/manual/security/) 4. Elasticsearch Shield(https://www.elastic.co/products/shield)

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw