資安威脅趨勢 - 中國駭客鎖定SonicWall的SSL VPN設備進行攻擊行動

- 3月 13, 2023

雲智維科技 Cloud Intelligent Operation, CIO

中國駭客鎖定SonicWall的SSL VPN設備進行攻擊行動

一、摘要

資安業者Mandiant揭露中國駭客組織UNC4540正在針對SonicWall的SSL VPN系統Secure Mobile Access(SMA)進行攻擊，其目的可能是竊取使用者的帳密資料。

二、存在風險

研究人員指出，駭客運用的惡意軟體，由名為TinyShell的後門程式，偽裝成防火牆組態設定程式的ELF可執行檔以及數個bash指令碼組成。另，駭客為了讓惡意程式可以持續在受害的SMA設備上運行，不僅採用備援機制，也竄改韌體植入後門root使用者帳號，且每10秒會偵測一次是否有遭到覆寫的狀況。

駭客主要目的是竊取使用者登入的帳號密碼資訊，其將透過firewalld這個bash腳本執行SQL指令"select userName, password from Sessions"取得數據並將數據儲存到/tmp/syslog.db，攻擊者取得數據後會採用離線方式破解加密密碼。

惡意檔案的Hash可參考下方圖表：

Path	Hash	Function
/bin/firewalld	e4117b17e3d14fe64f45750be71dbaa6	Main malware process
/bin/httpsd	2d57bcb8351cf2b57c4fd2d1bb8f862e	TinyShell backdoor
/etc/rc.d/rc.local	559b9ae2a578e1258e80c45a5794c071	Boot persistence for firewalld
/bin/iptabled	8dbf1effa7bc94fc0b9b4ce83dfce2e6	Redundant main malware process
/bin/geoBotnetd	619769d3d40a3c28ec83832ca521f521	Firmware backdoor script
/bin/ifconfig6	fa1bf2e427b2defffd573854c35d4918	Graceful shutdown script

建議改善措施：

1. 將SMA100更新至10.2.1.7或更高版本。
2. 將以上Hash情資同步至資安設備或是端點防護進行聯防。

情資報告連結：https://www.mandiant.com/resources/blog/suspected-chinese-persist-sonicwall

資安威脅趨勢 SonicWall SSL VPN

這個網誌中的熱門文章

案例分享-某企業AD上百組帳號大量登入失敗導致鎖定事件
- 11月 22, 2022
某企業 AD 上百組帳號大量登入失敗導致鎖定事件 一、案例故事 某企業客戶於某日下午發生 Exchange 遭受外部惡意主機大量進行暴力破解攻擊，導致企業內部環境 AD 伺服器短時間內被鎖定一百多筆帳號事件，而該企業也有在 Exchange 的 WebMail 上啟用雙因子認證，還是在短時間內遭受大量暴力破解攻 …
閱讀完整內容
-->

案例分享-某企業內部潛在APT攻擊行為
- 12月 06, 2022
某企業內部潛在 APT 攻擊行為 一、 案例故事 某企業客戶於某日下午發生內部主機有大量連線惡意網域事件，該客戶使用防毒軟體掃描後並無發現任何異常，經過深入調查發現該主機已被植入相關代理 / 連線程式進而成為駭客所操控的主機 / 跳板之一，而該代理 / 連線程式皆屬於合法程式，因此防毒軟體無 …
閱讀完整內容
-->

漏洞分享 - FortiOS SSL-VPN 中存在Heap緩衝區溢位漏洞(CVE-2022-42475)
- 12月 14, 2022
FortiOS SSL-VPN 中存在 Heap 緩衝區溢位漏洞 一、 摘要 FortiOS SSL-VPN 中 Heap 緩衝區溢位漏洞 [CWE-122] (CVE-2022-42475) 允許未經 身份驗證的遠端攻擊者可以透過請求來執行任意程式或指令。
閱讀完整內容
-->

漏洞更新 - Samba 釋出安全更新
- 12月 17, 2022
Samba 釋出安全更新 一、 摘要 Samba數個版本存在多種漏洞，其將允許駭客利用這些漏洞後控制系統。
閱讀完整內容
-->

案例分享-某企業專業IDC機房MS-SQL伺服器橫向感染入侵內部重要設備
- 12月 05, 2022
某企業專業 IDC 機房 MS-SQL 伺服器橫向感染入侵內部重要設備 一、案例故事 某企業客戶於某日下午在專業IDC機房中的MS-SQL伺服器透過VPN連線發起對內部OA網段、IT人員主機、防火牆、網路設備進行大量掃描探測行為，同時該主機也頻繁的對骨幹網路上的重要設備(防火牆、Switch、AD/DNS …
閱讀完整內容
-->

案例分享 - 某企業專業IDC機房VPN用戶帳號密碼外洩導致合法入侵VPN服務並進到內網
- 3月 23, 2023
某企業專業IDC機房VPN用戶帳號密碼外洩導致合法入侵VPN服務並進到內網 一、案例故事 某企業客戶於某日晚上10至凌晨1點在專業IDC機房中的VPN設備遭到駭客入侵，其駭客透過某一帳號成功登入VPN，取得授權後的攻擊者，利用VPN連線發起對內部OA網段、IT人員主機和網路設備以及DNS伺服 …
閱讀完整內容
-->

案例分享-某企業內部潛藏中毒主機，企圖橫向感染重要伺服器以及暴力破解嘗試入侵NAS網路儲存伺服器
- 12月 12, 2022
某企業內部潛藏中毒主機，企圖橫向感染重要伺服器 以及暴力破解嘗試入侵NAS網路儲存伺服器 一、案例故事 某企業客戶於某連假下午發生內部中毒主機意圖橫向感染其他主機，該台中毒主機對目的設備192.168.0.x【防火牆】和192.168.0.x【NAS】進行掃描探測，其目的是為瞭解該設備開啟哪些通 …
閱讀完整內容
-->

漏洞更新 - Adobe釋出數個產品的安全漏洞更新
- 1月 11, 2023
Adobe釋出數個產品的安全漏洞更新 一、 摘要 Adobe釋出Adobe Acrobat、Adobe Reader、Adobe InDesign、Adobe InCopy和Adobe Dimension等產品的安全漏洞更新。
閱讀完整內容
-->

漏洞分享 - 全景軟體 ServiSign跨平台數位簽章存在漏洞 (CVE-2022-46306、CVE-2022-46305、CVE-2022-46304)
- 12月 16, 2022
全景軟體 ServiSign跨平台數位簽章存在漏洞 (CVE-2022-46306、CVE-2022-46305、CVE-2022-46304) 一、 摘要 全景軟體 ServiSign跨平台數位簽章存在Path Traversal、Command Injection漏洞。
閱讀完整內容
-->

案例分享-某企業環境網路設備異常緩慢，導致內部使用者網路品質不佳
- 12月 08, 2022
某企業環境網路設備異常緩慢 導致內部使用者網路品質不佳 一、 案例故事 某企業客戶於某日上午發現其網路異常緩慢、掉包狀況，嚴重影響企業內部使用者的網路使用品質，該企業透過「雲智維資訊顧問代管代維方案」快速發現到是其內部某台網路設備有大量掉包及 ICMP response 延遲非常高的情形，以 …
閱讀完整內容
-->