TLP:CLEAR

設計安全

調整網絡安全風險平衡：

「設計安全軟件」
的原則和方法

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

目錄

概述：
設計漏洞

隨著面向互聯網的系統與直接影響我們經濟繁榮、生計甚至健康的關鍵系統，從個人身份管理到醫療保健等方面的連接日益緊密，科技已經融入到日常生活的幾乎每個方面。這些便利的一個負面例子是網絡漏洞已導致全球範圍內的醫院取消手術並轉移患者照護。關鍵系統中的不安全技術和漏洞可能會招致惡意網絡入侵，從而導致潛在的安全[1]風險。

因此，技術製造商非常有必要將「設計安全」和「預設安全」作為產品設計和開發流程的重點。一些供應商在推動軟件保障行業向前發展方面取得了長足進步，而另一些供應商則落後了。編寫機構強烈建議每家技術製造商都基於減輕客戶的網絡安全負擔建立其產品，包括防止客戶不得不不斷進行監控、例行更新和系統損壞控制以減輕網絡入侵。我們還敦促軟件製造商以有助於自動配置、監控和例行更新的方式建立其產品。我們鼓勵製造商承擔改善其客戶安全結果的責任。過去，技術製造商一直依賴於修復客戶部署產品後發現的漏洞，要求客戶自費應用這些補丁。只有結合「設計安全」實踐，我們才能打破創建和應用修復程序的惡性循環。**注意：**「設計安全」這個術語包括設計安全和預設安全兩者。

為實現這種高標準的軟件安全，編寫機構鼓勵製造商優先考慮將產品安全融合作為功能和上市速度的關鍵先決條件。隨著時間的推移，工程團隊將能夠建立一種新的穩態節奏，在這種節奏中，安全性真正融入設計之中，並且需要較少的維護。

反映這一觀點，歐盟在 網絡韌性法案 中強調了產品安全的重要性，強調製造商應在產品的整個生命週期實施安全措施，以防止製造商將有漏洞的產品引入市場。

[1] 編寫機構認識到，「安全」一詞根據其使用的上下文具有多種含義。在本指南中，「安全」是指提高技術安全標準以保護客戶免受惡意網絡活動的侵害。

為了創造一個技術和相關產品對客戶來說更安全的未來，編寫機構敦促製造商改進他們的設計和開發計劃，只允許向客戶提供設計安全和預設安全的產品。在開發之前，設計安全的產品是指將客戶安全作為核心業務目標，而不僅僅是一個技術功能的產品。設計安全的產品在開發開始之前就以該目標為出發點。現有產品可以在多次迭代中演變為設計安全狀態。預設安全的產品是那些「開箱即用」的安全產品，幾乎或完全不需要更改配置，並且無需額外費用即可獲得安全功能。這兩個原則共同將保持安全的大部分負擔轉移給了製造商，並減少了客戶因配置錯誤、補丁速度不夠快或許多其他常見問題而成為安全事件受害者的可能性。

網絡安全和基礎設施安全局 (CISA)、國家安全局 (NSA)、聯邦調查局 (FBI) 和以下國際合作夥伴[2]提供本指南中的建議，作為技術製造商確保其產品安全的路線圖：

- 澳洲網絡安全中心 (ACSC)
- 加拿大網絡安全中心 (CCCS)
- 英國國家網絡安全中心 (NCSC-UK)
- 德國聯邦資訊安全辦公室 (BSI)
- 荷蘭國家網絡安全中心 (NCSC-NL)
- 挪威國家網絡安全中心（NCSC-NO）
- 紐西蘭電腦應急響應小組（CERT NZ）和紐西蘭國家網絡安全中心（NCSC-NZ）
- 韓國互聯網與安全局（KISA）
- 以色列國家網絡總局（INCD）
- 日本國家網絡安全事件準備和戰略中心（NISC）和日本電腦應急響應小組協調中心（JPCERT/CC）
- OAS/CICTE美洲政府網絡事故應對小組（CSIRT）
- 新加坡網絡安全局（CSA）
- 捷克共和國國家網絡和資訊安全機構（NÚKIB）

編寫機構承認許多私營部門合作夥伴在推進設計安全和預設安全方面的貢獻。本產品旨在推動國際間有關關鍵優先事項、投資和決策的對話，這些對話是實現技術在設計和預設情況下安全、可靠和有韌性的未來所必需的。為此，編寫機構徵求相關各方對此產品的反饋，並打算召開一系列聆聽會議，以進一步完善、明確和推進我們的指南，以實現我們的共同目標。

有關產品安全重要性的更多資訊，請參閱 CISA 的文章，《不安全技術的代價以及我們能做些什麼》。

[2] 以下簡稱「編寫機構」。

最新消息

此報告的初次發布在軟件行業內引起了廣泛的討論。每天都有機構和個人受到威脅的消息，這突顯了就如何解決軟件產品中的長期和系統性問題進行更多討論的必要性。

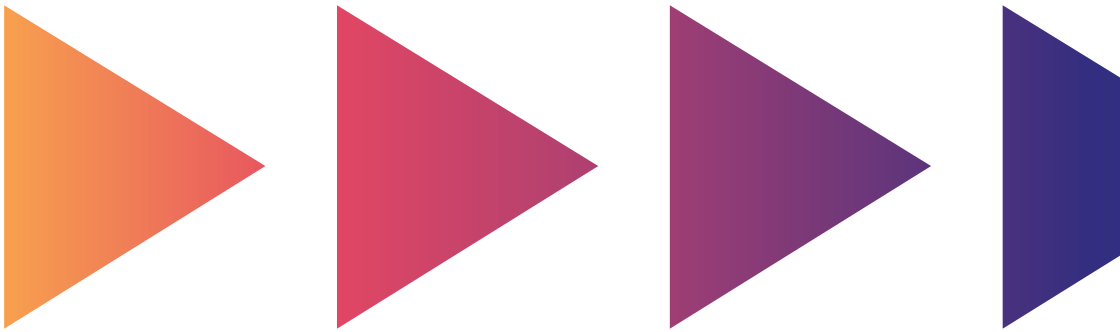
在2023年4月發布後，編寫機構（以下簡稱「我們」和「我們的」）收到了來自數百個個人、公司和行業協會的深思熟慮的反饋。反饋中最常見的請求是提供更多關於這三個原則如何適用於軟件製造商和他們的客戶的細節。在本文件中，我們擴展了原始報告並提及了如製造商和客戶的規模、客戶的成熟度以及原則範圍等其他主題。

軟件無處不在，任何一份報告都無法充分涵蓋軟件系統、軟件產品的開發、客戶的部署和維護，以及與其他系統的集成的全部內容。對於以下沒有明確映射到特定環境的指引，我們期待聽取社會各界對本文所述實踐如何導致特定安全改進的意見。

此報告也適用於人工智能（AI）軟件系統和模型的製造商。儘管它們可能與傳統形式的軟件有所不同，但基本的安全實踐仍然適用於AI系統和模型。一些安全設計實踐可能需要修改以考慮AI特定的考慮因素，但三個主要的安全設計原則適用於所有AI系統。

我們認識到，轉變軟件開發生命周期（SDLC）以符合這些安全設計原則並不是一項簡單的任務，可能需要時間。此外，規模較小的軟件製造商可能會難以實施其中許多建議。我們認為軟件行業需要普及那些使產品更安全的工具和程序。隨著越來越多的人和機構將注意力集中在軟件安全改進上，我們相信有創新的空間，可以縮小較大和較小的軟件製造商之間的差距，使所有客戶受益。

對最初的「設計安全」報告的更新，是我們致力於與支撐我們技術生態系統的眾多相互關聯的利益相關者社區建立夥伴關係的一部分。這是該生態系統許多部分的反饋的結果，我們將繼續聆聽和學習不同觀點。儘管前方有許多挑戰，但當我們對已經採用安全設計理念的人和機構有更多了解，並且獲知他們往往取得了成功時，我們對未來充滿樂觀。



如何使用本文件

我們敦促軟件製造商堅持本文件中的原則。軟件製造商可以根據以下步驟，通過公開記錄他們所採取的行動，以證明他們的承諾。我們鼓勵軟件製造商找到符合本原則精神的策略，並創造出產品，讓即使持懷疑態度的現有和潛在客戶也相信，他們體現了「設計安全」的理念。

除了軟件製造商應採取的行動外，客戶也可以利用本文件。購買軟件的公司應該向他們的供應商提出刁鑽的問題，借鑒本文件中列舉的堅持原則的例子。這樣，客戶就可以幫助將市場轉向更具設計安全的產品。CISA的《K-12技術採購指南》提供了客戶可以向供應商提問的示例。

我們鼓勵企業客戶將這些做法納入採購流程、供應商盡職調查評估、企業風險接受決策以及評估供應商時採取的其他步驟中。客戶還應推動供應商公開記錄每個供應商所採取的安全設計行動。總體而言，這可以創建一個強烈安全需求信號，從而鼓勵並促使軟件製造商採取措施提高安全性。換句話說，正如我們試圖在軟件製造商內部創建一種普遍的安全設計理念一樣，我們需要在其客戶中創建一種「需求安全」文化。

設計安全

「設計安全」是指技術產品的構建方式可以合理地防止惡意網絡行為者成功訪問設備、數據和連接的基礎設施。軟件製造商應執行風險評估，以識別和列舉對關鍵系統的普遍網絡威脅，然後在產品藍圖中包含保護措施，以應對不斷變化的網絡威脅情況。

安全資訊技術 (IT) 開發實踐和多層防禦（稱為深度防禦），亦被建議用來防止對手活動危害系統或未經授權獲取敏感數據。編寫機構進一步建議製造商在產品開發階段使用定制的威脅模型，以應對對系統的所有潛在威脅，並考慮每個系統的部署過程。

編寫機構敦促製造商對其產品和平台採取整體安全方法。設計安全的開發需要軟件製造商在產品設計和開發過程的每一層投入大量資源，這些資源不能在以後「附加」。這需要製造商最高業務主管的強有力領導，使安全作為業務優先事項，而不僅僅是一項技術功能。業務領導者和技術團隊之間的這種協作從設計和開發的早期階段延伸到客戶部署和維護。我們鼓勵製造商作出艱難的權衡和投資，包括那些對客戶「不可見」的，例如遷移到消除廣泛漏洞的編程語言。他們應該優先考慮保護客戶的功能、機制和工具的實施，而非那些看似有吸引力但會擴大攻擊面的產品功能。

沒有單一的解決方案可以結束惡意網絡行為者利用技術漏洞的持續威脅，「設計安全」的產品將繼續受到漏洞的影響；但是，大量漏洞是由相對較小的根源子集造成的。製造商應制定書面路線圖，以使其現有產品組合與更多「設計安全」實踐保持一致，確保僅在特殊情況下才會出現偏差。

編寫機構承認，為客戶承擔安全結果的責任並確保這種水平的客戶安全可能會增加開發成本。然而，在開發新技術產品和維護現有產品的同時投資於「設計安全」實踐，可以顯著改善客戶的安全態勢並降低遭受攻擊的可能性。「設計安全」原則不僅加強了客戶的安全態勢和開發者的品牌聲譽，而且長期來看降低了製造商的維護和補丁成本。

下面列出的「對軟件製造商的建議」部分提供了一個建議的產品開發實踐和政策清單，供製造商考慮。

預設安全

「預設安全」是指產品開箱即可抵禦普遍的漏洞利用技術，無需額外付費。這些產品可以抵禦最普遍的威脅和漏洞，而終端用戶無需採取額外的措施來保護它們。預設安全產品旨在讓客戶敏銳地意識到，當他們偏離安全預設值時，除非他們實施額外的補償控制，否則他們會增加遭受攻擊的可能性。預設安全是設計安全的一種形式。

- 安全配置應該是預設基線。預設安全產品會自動啟用保護企業免受惡意網絡行為者侵害所需的最重要的安全控制措施，並提供可使用和進一步配置安全控制措施的能力，無需額外費用。
- 安全配置的複雜性不應是客戶的問題。組織的IT人員經常因安全和運營責任而超負荷，從而導致有限時間來了解和實施強大的網絡安全態勢所需的安全影響和緩解措施。通過優化安全產品配置，即確保「預設路徑」，製造商可以通過確保他們的產品按照「預設安全」標準安全地製造、分銷和使用，來幫助他們的客戶。

「預設安全」產品的製造商不會為實施額外的安全配置收取額外費用。相反，他們將這些包含在基礎產品中，就像所有新車都配有安全帶一樣。

安全不是奢侈的選擇，而是更接近每個客戶應該期望的標準，而無須爭議或支付更多費用。

對軟件製造商的建議

本聯合指南為向製造商提供建議，以製定書面路線圖來實施和確保IT安全。編寫機構建議軟件製造商實施以下各節概述的策略，以通過設計安全和預設安全原則來承擔其客戶的安全結果。

軟件產品安全原則

我們鼓勵技術製造商採用優先考慮軟件安全的戰略重點。編寫機構制定了以下三個核心原則，以指導軟件製造商在開發、配置和交付其產品之前將軟件安全納入到其設計流程。

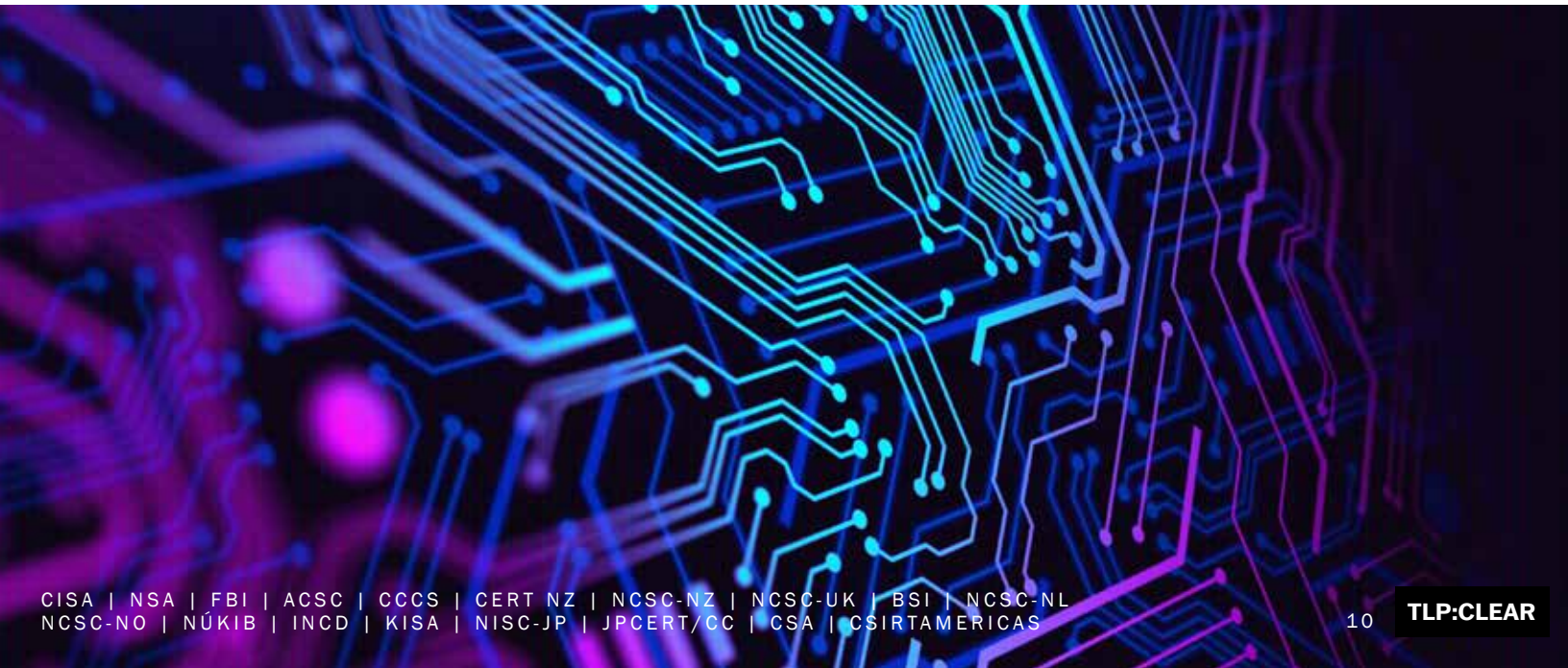
1 **對客戶的安全結果負責**，並相應地改進其產品。安全的責任不應只由客戶承擔。

2 **採用徹底的透明度和問責制。**

軟件製造商應該以提供安全可靠的產品為榮，並根據自己的能力在其他製造商群體中脫穎而出。這可能包括共享他們從客戶部署中了解到的資訊，例如採用強化身份驗證機制預設。還包括確保漏洞公告和相關的常見漏洞和暴露 (CVE) 記錄完整且準確的堅定承諾。但是，要提防將 CVE 視為負面指標的誘惑，因為這些數字也是健康的代碼分析和測試社區的標誌。

3 **建立組織結構和領導來實現這些目標。**

雖然技術專業知識對於產品安全至關重要，但高級管理人員是在組織中實施變革的主要決策者。高管層需要將安全作為機構產品開發的一個關鍵要素進行優先考慮，並且與客戶建立合作夥伴關係。



為了實現這三個原則，製造商應該考慮幾種操作策略來改進他們的開發流程。

定期與公司行政領導召開會議，以推動組織內設計安全和預設安全的重要性。應制定政策和程序來獎勵那些開發遵守這些原則的產品的生產團隊，其中可以包括對實施出色的軟件安全實踐的獎勵，或工作階梯和晉升標準的獎勵。

強調軟件安全對業務成功的重要性。例如，考慮指派一個堅持商業和 IT 實踐的「軟件安全負責人」或「軟件安全團隊」，以直接將軟件安全標準與製造商責任聯繫起來。製造商應確保他們的產品擁有穩健、獨立的產品安全測評和評估程序。

在資源分配和開發過程中使用定制的威脅模型，以優先考慮最關鍵和影響大的產品。威脅模型考慮到產品的具體使用情況，並使開發團隊能夠強化產品。最後，高層領導應將交付安全產品作為產品卓越和質量的關鍵因素，對團隊進行責任追究。

作為本指南2023年10月更新版的一部分，這三個原則通過以下解釋、演示和證據得到了進一步的闡釋。

原則 1：對客戶的安全結果負責

解釋

現代最佳實踐要求軟件製造商投資產品安全工作，包括**應用程式加固、應用程式功能，**以及應用程式**預設設置。**

軟件製造商需要通過使用能夠提高惡意行為者破壞應用程式的成本的程序和技術，來實施**應用程式加固**。應用程式加固的協定和程序有助於產品抵抗智能惡意行為者的攻擊。加固、產品安全和韌性等術語都與產品質量密切相關。我們的理念是安全必須是「內置的」，而非「附加的」。[1] 通過內置安全，軟件製造商不僅可以提高客戶的安全性，還可以提高產品質量。示例策略包括確保用戶輸入經過校驗和驗證，不直接輸入代碼（即使用參數化查詢），使用記憶體安全的編程語言，嚴格的軟件開發生命週期（SDLC）管理，以及使用硬件支持的加密密鑰管理。

應用程式需要支持與網絡安全相關**應用程式功能**。這些功能有時被稱為「能力」，可擴展產品或服務的功能，幫助客戶維護或提高客戶安全態勢。

與安全相關的功能示例包括支持所有網絡連接的傳輸層安全性（TLS），單點登錄（SSO）支持，多重要素驗證（MFA）支持，安全事件審計日誌，以角色為基礎的存取控制（RBAC）和基於屬性的存取控制（ABAC）。

這些產品功能中的一些是可配置的，允許客戶更輕鬆地將產品整合到其現有環境和工作流程中。這些配置意味著應用程式必須在客戶配置之前設置**預設設置**。這些預設設置需要在「開箱即用」的情況下安全地設置，以便客戶花費更少的資源來提高其技術產品堆棧的安全性。

應用程式加固、應用程式安全功能和應用程式預設設置中的每一個元素，都在應用程式的安全性和客戶的安全態勢方面都發揮著作用。軟件製造商應該思考這些元素及它們之間的關係。製造商應該考慮的不僅僅是將這些元素納入產品的投資。製造商應該更進一步，考慮這些元素如何改變客戶的現實安全態勢，無論是好還是壞。

製造商應該對客戶的安全結果負責，而不僅僅根據他們的努力和投資來衡量自己。應將責任放在上游，即製造商，這樣有最大可能降低遭受攻擊的機會。

遺憾的是，這在今天並非如此。太多製造商將安全的責任放在客戶身上，而不是投資於全面的**應用程式加固**。舉例來說，當製造商修補一個漏洞時，我們常常看到由於他們處理的是症狀而不是根本原因，類似的漏洞又暴露出來。產品可能在代碼庫的不同部分針對同一類型漏洞實施不同的緩解措施。舉例來說，在製造商修復了一個輸入驗證漏洞後，研究人員或攻擊者找到了未從改進的輸入驗證中受益的代碼路徑。製造商一次修復一個漏洞，而不是統一代碼庫以在整個應用程式中消除該類漏洞。

應用程式功能對客戶來說既帶來利益又帶來風險。允許與許多外部系統和版本集成的功能可以大大提高產品的價值。然而，如果客戶缺乏對持續使用該功能的理解，那麼支持沒有退役計劃的功能（如網絡協議）可能會使客戶容易受到威脅。例如，一些產品仍在使用起源於1990年代或2000年代的網絡協議，這些協議現在已經被認為是不安全的。有很多因素可能減緩客戶升級並部署現代安全措施的速度。他們可能使用與機構網絡的其他部分集成的產品，但這些產品缺乏現代安全措施，使得IT團隊無法進行現代化。儘管如此，軟件製造商仍可在其規劃流程中考慮這些模式，以鼓勵客戶與時俱進。

應用程式預設設置是客戶潛在風險的新增領域。製造商通常選擇某些預設設置，使客戶更容易使用他們想要的應用程式功能。缺點是，這種做法增加了客戶攻擊面，因為他們可能並不需要預設啟用某些功能和協議。此外，許多安全控制都是預設關閉的，或者要求客戶花時間配置其設置以提高安全性。明確的威脅模型是一種策略，可以幫助決定哪些功能應該預設啟用，或者哪些設置應該需要預設安全。另一種策略是研究如何使功能更容易被管理員發現。

一些製造商出貨的產品的預設設置可能對部分或全部客戶帶來風險。與其設置更安全的預設設置，他們通常選擇製作**加固指南**，客戶必須自費實施。加固指南存在一些常見問題。有些加固指南很難找到，並且得不到很好的支持。有些實施起來復雜，有時需要軟件開發人員來編寫擴展模塊。還有一些假設讀者擁有豐富的網絡安全經驗，能夠理解各種設置改變攻擊面的方式。對攻擊者的工作方式了解不全面的從業人員可能無法正確實施加固指南的指示，尤其如果指南中的指示沒有明確說明權衡取捨。而且，並非所有的加固指南都是由深入了解攻擊者戰術和經濟因素的工程師編寫的，這就導致他們編寫的加固指南即使忠實實施也無法無效。數以百萬計的客戶正在承擔加固多個軟件或系統實例的責任，而且通常是在資源受限的環境中。依賴加固指南根本無法具有規模性。

無論應用程式的設置是預設的還是由客戶設置，都應根據製造商對威脅狀況的當前理解進行持續評估。應用程式應明確顯示這些設置可能導致的潛在風險，並將這些指標公之於眾。就像現代汽車有一個安全帶指示器，如果你不佩戴安全帶開車，汽車就會發出警報，軟件也應該有系統安全狀態的指示器。如果應用程式配置為不需要管理員帳戶的MFA，應該定期提醒管理員，如果他們不配置MFA，他們和整個機構都會處於危險之中。此外，如果一個應用程式被配置為支持舊協議，而現在已知這些協議實施了薄弱的加密技術，那麼它就應該定期向管理員說明組織處於危險之中並提供資源解決這種情況。我們敦促製造商實施內置於產品中的常規提示，而不是依賴管理員有時間、專業知識和意識來解釋加固指南。在平衡安全性和可用性方面，顯然存在創新機會。

以上每個元素都創造了一種難以維持的局面，即客戶需要研究、資助、購買、配備人員、部署和監控額外的**安全產品**，以降低遭受攻擊的機會。中小型機構（SMO）通常無法獲得這些選擇。他們面臨專業知識、資金和時間的匱乏，這就給寬頻和功能造成了負擔，迫使安全性降至較低優先程度，並在整體上加劇了集體風險。相反，相對較少的製造商的安全投資將具有規模效益。總結這個問題的一句常用語是：軟件行業需要更安全的產品，而不是更多的安全產品。軟件製造商應引領這一轉變。

> ***軟件行業需要更安全的產品，而不是更多的安全產品。軟件製造商應引領這一轉變。***

如今，我們有時會看到製造商在評論中解釋說，由於未啟用特定安全功能或遵循特定的加固指南而導致客戶遭受攻擊。相反，在客戶遭受攻擊後，製造商應該解釋特定的安全功能或特定的加固指南是否可以防止攻擊，並考慮免費將其作為預設設置。如果產品本身在設計和實施階段沒有充分加固，製造商應該解釋他們正在如何努力從產品線中消除這類漏洞。

軟件製造商有責任確保他們的產品以安全性為首要目標進行設計和開發。為此，他們應該**客觀衡量**他們在實際應用中的努力結果。我們呼籲製造商不僅要關注內部工作，還要客觀地衡量和定期報告產品安全工作和配置的結果和有效性，並建立一個反饋迴路，促使SDLC中的變化，從而為客戶安全和更安全的產品帶來可衡量的改進。報告應包括匿名化的數據，供學術界和安全研究社區使用，以跟蹤高層次趨勢並在整個生態系統中測量進展。

展示此原則

軟件製造商和在線服務應尋找展示實施此原則成功的方式。他們應該設法以產品的形式提供證據，供外界檢查。沒有任何一件產品可以單獨證明製造商正在實施穩健的安全設計計劃，但通過提供各種產品，可以證明製造商致力於開發安全產品。這種方法符合「展示而非講述」的精神。

為展示此原則，軟件製造商應考慮採取以下清單中的步驟。編寫機構認識到，很少有軟件製造商能夠在其安全設計之旅一開始就立即實施這些實踐並生成相應的產品。此外，軟件製造商將需要根據客戶在現場部署產品的方式來確定此清單的優先順序，以獲得最大的安全效益。

預設安全實踐

1. **消除預設密碼。**預設密碼仍然被認為是每年許多攻擊的罪魁禍首。承諾消除這個長期問題將阻止攻擊者輕易存取。同樣，製造商應考慮應該實施哪些密碼實踐，如最短密碼長度和禁止使用已知被破解的密碼。

2. **進行現場測試。**隨著技術不斷演進且變得更加複雜，軟件製造商越來越有必要進行以安全為中心的用戶測試，以了解其產品在現場的安全狀況。與用戶研究為軟件開發需求提供資訊類似，軟件製造商也應進行以安全為中心的用戶研究，以了解安全用戶體驗（UX）的不足之處。通過觀察客戶在實際環境中如何部署和使用產品，軟件製造商可以獲得有價值的見解，了解其安全功能和控制的可用性和效果。這些見解可以幫助確定需要改進的地方，並改進產品以更好地滿足客戶的安全需求。例如，現場測試可能會建議更改用戶體驗流程、預設值、警報和監控。現場測試還可以顯示產品設計中哪些過去的改進，減緩了安全補丁的速度，減少配置錯誤，並最小化攻擊面。

製造商應考慮以下事項：

- 客戶是否正確實施了加固指南？
- 產品現有的安全功能在實際應用的表現是否符合預期？
- 這些功能是否真的能夠抵抗現實世界中的攻擊？
- 哪些功能可以更好地減少遭受攻擊的可能性？

注意：為了更深入地了解這些元素，軟件製造商可能希望與客戶合作進行紅隊演習，以了解產品如何抵抗攻擊。這些現場測試可以在客戶的實際場地、虛擬場地或以保護隱私的方式通過應用程式的遙測進行。

3. **縮小加固指南的規模。**製造商可以通過簡化或甚至取消產品加固指南，專注於客戶在部署產品時應優先考慮的最關鍵的安全措施，來提高客戶的安全態勢。相對於向客戶提供一系列的安全措施，製造商應該識別其產品容易受到的首要安全風險，並提供清晰簡明的指導，說明如何減輕這些風險。此外，製造商還應該為客戶提供簡化安全控制實施過程的工具和自動化手段，例如可在客戶環境中輕鬆部署的腳本。這些工具還應能夠驗證並清楚顯示從原始基準線所做的更改。通過簡化加固指南並為客戶提供易於使用的工具和自動化手段，製造商可以減輕客戶的負擔，並有助於確保其產品以安全的方式部署。一種策略是考慮實施帕累托原則，以減少常見用例（80%）的步驟，然後為不太常見情景（20%）提供情境指導和工具。通過這種方式，軟件製造商就能化繁為簡、化難為易。現場測試將是衡量客戶發現、理解和實施加固指南所需時間的有力工具。製造商應該考慮產品如何在產品中引導管理員採取行動，而不是依賴管理員執行加固指南中的任務。

4. 積極阻止使用不安全的遺留功能。

優先通過明確的升級路徑，而非向後兼容性提升安全性。發布博客，展示採用更安全功能和協議的情況，並通過公告（可能從產品內部）廢除不安全的功能。相當多的客戶已經證明，他們不會使其系統與現代網絡、身份和其他關鍵安全功能保持最新。在某些情況下，客戶擔心升級會使現有功能中斷。通過盡可能實現無縫升級，客戶可能會更頻繁且更快地進行升級並獲得安全修復。軟件製造商應該積極引導客戶進行升級，以降低客戶風險。

5. 實施引人注意的警報。

類似於汽車的安全帶警報在未係安全帶時會持續發出聲音，當用戶或管理員處於真正不安全的狀態時，製造商應實施及時且重複的警報，警告管理員在其環境中使用過時的協議並建議升級路徑。當用戶或管理員，或應用程式配置處於不安全狀態時，及時且重複的發出警報。定期讓管理員了解不安全模式。還可以增加一項功能，要求超級管理員在每次登錄時確認其帳戶沒有MFA，甚至在啟用MFA之前禁用某些關鍵功能。要實現這些目標，同時不引起警報疲勞，還需要一些創新。

6. 創建安全配置模板。

這些模板可以根據組織的風險態度，預設某些配置為安全設置。雖然低/中/高安全性模板可能過於簡單，但這個例子說明了可以更新多少設置來管理組織風險。模板可以由製造商確定的風險加固指南提供支持。

安全產品開發實踐

1. **記錄與安全SDLC框架的一致性。**安全SDLC框架提供跨人員、流程和技術的目標和示例。考慮發布關於已實施的安全SDLC框架控制的詳細說明，並描述已使用的任何替代控制措施。在美國，考慮使用NIST安全軟件開發框架（SSDF）。儘管SSDF並非檢查清單，但它「描述了一套用於安全軟件開發的基本、合理的實踐。」

2. **記錄網絡安全性能目標（CPG）或同等一致性。**當一個機構宣稱他們符合NIST SSDF標準時，即表明他們的SDLC遵循了廣為人知的最佳實踐。然而，僅擁有堅固的SDLC是不夠的。他們還需要保護自己的企業和開發環境，防止惡意行為者在產品仍在開發階段時試圖操縱產品的安全屬性。這不是一種理論上的攻擊，而是一種已經實施並對客戶造成不利的攻擊，進而危及國家安全。各機構應考慮公布本機構符合CISA CPG、NIST網絡安全框架（CSF）或其他網絡安全計劃框架的詳細資訊。

3. **漏洞管理。**一些製造商的漏洞管理程序只關注修補內部或外部發現的漏洞，僅此而已。更成熟的程序會對漏洞及其根本原因進行廣泛的數據驅動分析，採取步驟來系統性地消除整個漏洞[3]。他們圍繞設定質量計劃、質量控制、質量改進和質量測量實施正式程序。他們將缺陷管理視為業務問題，而不僅僅是一個安全問題。在某些方面，這些程序與其他行業的質量和安全程序並無二致。

4. **負責任地使用開源軟件。** 在使用開源軟件時，應通過審查開源包、促進代碼貢獻回歸依賴項，並幫助維持關鍵組件的開發和維護來承擔責任。作為參考，日本經濟產業省（METI）發布了「利用OSS並確保其安全性的管理方法的用例示例集」。

5. **為開發人員提供安全的預設值。** 通過為開發人員提供安全的構建塊，使軟件開發的預設路徑成為安全路徑。例如，鑑於SQL注入漏洞引起的現實危害十分普遍，應確保開發人員使用維護良好的庫來防止該漏洞類型。這種做法被稱為「鋪平道路」或「光明大道」，既能確保速度和安全性，又能減少人為錯誤。

6. **培養了解安全性的軟件開發人員隊伍。**通過培訓軟件開發人員掌握安全編碼的最佳實踐，確保他們了解安全性。此外，通過更新招聘實踐以評估安全知識，並與大學、社區學院、短期培訓班和其他教育機構合作，將安全性納入電腦科學和軟件開發課程中，從而幫助改造更廣泛的勞動力。

[3] NIST SSDF，PO 1.2，示例2：「定義指定組織軟件安全要求的政策，並在SDLC的關鍵點驗證合規性(例如，由閘口驗證的軟件缺陷類別、對發布的軟件中發現的漏洞的響應)。」

7. **測試安全事件事件管理（SIEM）與安全協調、自動化和響應（SOAR）集成。**除了進行現場測試外，還應與普及的SIEM和SOAR提供商以及選定的客戶一起合作，了解事故響應團隊如何使用日誌調查可疑或實際的安全事件。很少軟件開發人員有應對事故的經驗，因此他們創建的日誌條目對響應人員的幫助可能不如預期。通過與SIEM和SOAR技術以及真實的事故應對專業人員合作，開發團隊可以創建正確、完整的日誌，從而節省時間並減少事故中的不確定性。

8. **與零信任架構（ZTA）保持一致。**使產品部署指南與例如NIST ZTA模型和CISA零信任成熟度模型保持一致。鼓勵客戶在其環境中採用這些原則。

支持安全的業務實踐

1. **免費提供日誌記錄。**雲服務應承諾以免費形式生成和存儲與安全相關的日誌。本地部署產品應同樣以免費形式生成與安全相關的日誌。此外，由於許多客戶可能在事故發生後才了解其價值，因此產品應預設記錄安全事件。這些策略可能需要對以下方面進行徹底審閱：應該記錄哪些安全事件以提供網絡安全狀態意識、客戶可以如何配置日誌記錄、日誌保留的時間範圍是多少、如何保護日誌的完整性和存儲，以及如何分析日誌。在某些情況下，審閱結果可能會建議需要對應用程式的日誌管理架構進行重構，以幫助使日誌有可操作性，並降低製造商成本。與事故響應（IR）專家合作可以增加日誌對現場調查人員有用的機會。參見SIEM部分。

2. **消除隱性稅費。**發表承諾永不收取安全或隱私功能或集成的費用。例如，在身份和存取管理（IAM）的更大範圍內，有一種服務被稱為單點登錄（SSO）服務。有些製造商將其系統連接到SSO服務（有時稱為身份提供商）時，會收取更高的費用。這種「SSO稅」對於許多中小企業來說，意味著良好的身份和存取管理是難以實現的，阻礙了他們實現強大的安全態勢。有些服務為用戶啟用MFA時會收取更高的費用。**安全不應是奢侈品，而應被視為客戶的權利。**有些製造商認為，很少有客戶要求提供這些功能，而且這些功能的維護成本更高。這些論點忽略了一個事實，即很少有客戶會打電話投訴或討價還價，不是所有客戶都真正了解這些功能的好處，而且所有功能都有一定的維護成本。然而，我們並沒有看到多少製造商為可用性或數據完整性額外收費。支持這些關鍵屬性的成本已包含在所有客戶支付的價格中，就像在事故中挽救生命的安全帶、折疊式轉向管柱和安全氣袋的成本包含在汽車價格一樣。

3. **接受開放標準。**實施開放標準，尤其是在通用網絡和身份協議方面。在有開放標準可用時，避免專有協議。

4. **提供升級工具。**許多客戶不願意採用產品的最新版本，包括部署更新和更安全的功能，如安全網絡連接。軟件製造商可以通過提供工具來幫助減少不確定性和風險，從而提高客戶對新升級的採用。為客戶提供免費許可證，讓他們在測試環境中測試升級和補丁，作為激勵客戶的一種方式。

原則2：採用徹底的透明度和問責制

解釋

軟件製造商應該以提供安全可靠的產品為榮，並根據自己的能力在其他製造商群體中脫穎而出。

讓我們來談談一個有關透明度的常見擔憂。當從業者討論徹底的透明度時，往往會陷入一種擔憂，即他們在為「攻擊者提供路線圖」。然而，大量證據表明，攻擊者在沒有這種路線圖的情況下也做得到，應該打消這種擔憂，因為透明度能造福直接客戶、間接客戶、供應鏈和整個軟件行業。

透明度有助於行業建立慣例，換句話說，就是明確了「好」是什麼樣子。它有助於這些慣例隨著時間的推移而改變，以應對客戶需求、威脅行為者戰術或經濟的變化，或技術的演進。透明度有助於資源較少的製造商向那些資源更豐富和能力更強大的製造商學習。有關資訊共享的對話應該擴展到實時威脅指標之外，包括以下要素。

透明度迫使在開發過程盡早做出與安全有關的決策，並使之成為企業領導以及工程師和安全專業人員的持續活動。透明度可為產品建立問責制。

關於在「透明度」一詞前選擇「徹底」這一形容詞的說明。如今，軟件製造商很少公布他們如何開發和維護軟件，以及如何利用長期數據使程序成熟的詳細資訊。在軟件行業，很少有製造商提供有關如何設計其軟件的導覽。軟件製造商也很少有機會了解同行機構是如何構建其SDLC程序的，以及這些程序是如何抵禦真實攻擊者的。更多的資訊共享將使整個行業受益匪淺，例如衡量安全缺陷成本和消除漏洞類別的策略。由於這些常見的做法，每個軟件製造商都必須學會如何處理產品安全問題。也許通過不對安全功能收取奢侈稅，安全和安保就會以成本為中心而不是利潤為中心，公司將通過合作和透明度來減輕負擔，從而受益。

我們希望專注於能夠顯著加速軟件產業發展的策略。我們不能再投機取巧、循序漸進地改進了。如果我們要共同克服聰明和適應性強的對手帶來的威脅，我們必須接受這種今天讓人感到不適的透明度水平，但這將推動產業向前發展。如今，有些製造商已經體現了其中一些安全設計原則。正如威廉·吉布森（William Gibson）所說，「未來已經到來，只是分布得不太均勻。」**徹底的透明度將有助於傳播這些訊息，並使捍衛者比我們的對手受益更多。**

透明度不僅可以幫助同行機構成熟其SDLC。潛在客戶和投資者可以更了解製造商所做的投資和權衡，以及這些投資為客戶創造的安全態勢。接受徹底透明化的製造商將向客戶提供資訊，幫助他們做出購買決策，不僅根據價格和功能，還根據安全性。

儘管機構努力保護其供應鏈和SDLC，但最近仍有公司的構建流程遭受了攻擊。要實現徹底透明化，就必須公開披露攻擊事件，以及公司為預防和偵測未來攻擊所做的改進。這種形式的資訊共享將有助其他機構學習，避免遭受同樣的命運。

展示這項原則

為展示這項原則，軟件製造商應採取以下步驟：

預設安全實踐

1. **發布與安全相關的綜合統計數據和趨勢。**範例主題包括客戶和管理員採用 MFA 以及使用不安全的遺留協定的情況。
2. **發布補丁統計數據。**詳細說明使用該產品最新版本的客戶所佔的百分比，以及你正在採取哪些措施來使更新更輕鬆、更可靠。
3. **發布未使用權限的數據。**發布有關整個客戶群中過多權限的匯總資訊，以及為減少客戶的攻擊面而對產品所做的推動和其他更改。這些未使用的權限很可能為管理員敲響警鐘，就像安全帶提示音。

安全產品開發實踐

1. **建立內部安全控制。**許多公司已經看到將資料轉移到雲端提供商的好處。現在這些雲端提供商成為攻擊者的目標。軟件即服務 (SaaS) 提供商應公布其內部控制的統計數據。例如，SaaS 供應商應公布有關其內部部署的防網絡釣魚 MFA，如線上快速身份 (FIDO) 驗證的統計數據。理想情況下，他們應該能夠保證，如果未通過防網絡釣魚 MFA 身份驗證，任何員工都無法讀取客戶或其他敏感數據。

2. **發布高級威脅模型。**設計安全的產品首先要有書面威脅模型，描述創建者要保護的內容以及免受誰的攻擊。有效的威脅模型是參考野外發生入侵的方式，並應涵蓋企業和開發環境，以及軟件製造商希望其在客戶環境中使用的方式。

3. **發布詳細的安全 SDLC 自我測試。**遵循 NIST SSDF 或其他類似框架的製造商正在積極致力於成熟的軟件開發生命週期。發布製造商已實施哪些控制措施以及針對哪些產品的自我證明，將表明其致力於遵守這些最佳實踐，並增強客戶的信心。例如，其他認證計劃包括以色列網絡供應鏈方法等。

4. **接受將漏洞透明化。**發布承諾，確保已識別的產品漏洞將作為正確且完整的 CVE 條目發布。對於識別漏洞根本原因的通用缺陷列表欄位尤其如此。公共 CVE 資料庫越正確、越完整，業界就越能追蹤產品如何變得更加安全，以及哪些類別的漏洞最普遍。但是，請謹防將 CVE 視為負面指標的誘惑，因為此類數字也是代碼分析和測試社群健康發展的標誌。隨著製造商實施安全設計理念，由於對現有代碼中的漏洞進行更全面的發現和修復，他們的原始 CVE 數量一開始可能會增加。製造商應公布對過去漏洞的分析，包括為解決整類漏洞而採取的任何模式和措施。例如，如果一家公司的 CVE 很大一部分與跨站腳本 (XSS) 相關，那麼將根本原因分析、應對措施（例如轉向防止 XSS 的 網頁模板框架）和結果記錄在案，將向客戶表明他們不會受到這類幾十年前就有緩解措施的漏洞的傷害。

5. **發布軟件物料清單 (SBOM)。**製造商應掌控其供應鏈。各機構應該為每種產品建立和維護 SBOM [2]，向供應商索取數據，並使 SBOM 可供下游客戶和使用者使用。這將有助於展示他們在了解產品製造過程中使用的組件方面的努力，以及他們應對新發現風險的能力，並可以幫助客戶了解如果供應鏈中的某個模塊存在新發現的漏洞，應如何應對。作為參考，日本經濟產業省 (METI) 發布了

「軟件管理的軟件物料清單 (SBOM) 引入指南」。透明度應擴展到嵌入式設備中的固件以及人工智能/機器學習 (ML) 中使用的數據和模型。除了協助採購決策和營運能力之外，SBOM 在偵測和應對惡意供應鏈攻擊的基礎設施中發揮重要作用。

6. **發布漏洞披露政策。**發布漏洞披露政策，(1) 授權對製造商提供的所有產品以及這些測試的條件進行測試；(2) 為按照該政策執行的操作提供法律安全港；(3) 允許在設定的時間期限後公開披露漏洞。製造商應對已發現的漏洞進行根本原因分析，並在最大可行範圍內採取行動消除整個漏洞類別。請參閱 CISA 的漏洞揭露政策模板以取得參考語言。

支持安全的商業實踐

1. **公開提名一位設計安全高層執行發起人。**在許多機構中，安全性（如品質）被委託給技術團隊，而這些技術團隊進行結構改革以顯著提高產品安全性的能力有限。公開任命一位高級業務主管來監督設計安全計劃將使產品的安全性轉變為頂級商業關注問題。

2. **發布設計安全路線圖。**製造商應記錄為提高客戶安全性，而對其 SDLC 所做的更改，包括有關現場測試報告、為消除整類漏洞而採取的措施以及其他原則中列出的其他項目的詳細資訊。與質量改善工作一樣，安全改善計畫也有不同的規劃、控制和改進階段。本著展示而不只是講述的精神，公布這些階段背後的路線圖和細節將建立人們對產品設計安全的信心。在取得有意義的進展後，製造商可以在透明度報告中詳細說明這些進展。這樣做不僅表明了對設計安全原則的承諾，而且可以透過展示存在的證據，來激勵其他人採用類似的程序。

3. **發布記憶體安全路線圖。**製造商可以採取措施，透過遷移現有產品並使用記憶體安全語言建立新產品來消除最大的漏洞類別之一。雖然這可能並非在所有情況下都是可行的，但製造商可以考慮使用記憶體安全語言開發應用程式包裝器，而不是重寫整個應用程式。這還可以包括製造商如何更新招募、培訓、代碼審查和其他內部流程，以及他們如何幫助開源社群做同樣的事情。

4. **發布結果。**在更新其 SDLC 以體現安全設計理念時，機構會發現快速獲勝、資源密集型勝利以及一些意想不到的挫折。透過展示他們的內部成功和障礙，整個產業都可以從結果中學習。

原則 3：自上而下

解釋

雖然整體理念被稱為「設計安全」，但對客戶安全的激勵措施早在產品設計階段之前就開始了。它們從業務目標、以及隱含和明確的目標以及期望的結果開始。只有當高層領導者將安全作為業務優先事項、創造內部激勵並培養一種將安全作為設計要求的全面文化時，才能取得最佳結果。

雖然技術主題專業知識對於產品安全至關重要，但這並不是一個可以完全留給技術人員的問題。這是一個必須從高層開始的企業優先事項。

有些人不禁會問，如果軟件製造商已經接受前兩個原則並生產有意義的產品，那麼第三個原則是否必要？公司如何建立其願景、使命、價值觀和文化將影響產品，而這要素在公司高層佔據著重要的比重。我們在其他在安全和品質方面取得了顯著進步的行業中也看到了這一點。著名質量專家 J.M. Juran 寫道：

> ***要實現質量領導力，高層管理者必須親自負責質量管理。在實現質量領導力的公司中，高層管理者都會親自指導該計劃。據我所知，沒有任何例外。[3]***

我們認為安全是產品質量的一個子類別。當安全和質量成為企業的當務之急，而不是僅由技術人員承擔的技術職能時，機構將能夠更快、更有效率地回應客戶的安全需求。此外，投入必要的資源以確保軟件安全從一開始就成為核心業務優先事項，將降低解決軟件缺陷的長期成本，進而降低國家安全風險。

正如領導團隊實施企業社會責任 (CSR) 計劃一樣，人們越來越認識到，包括軟件製造商在內的企業董事會應在指導網絡安全計劃方面發揮更積極的作用。企業網絡責任 (CCR) 一詞有時用於描述這一新興理念。

展示這項原則

為了展示這項原則，軟件製造商應採取以下步驟：

1. **在公司財務報告中包含設計安全計劃的詳細資訊。**如果製造商是一家上市公司，則應在每份年度報告中加入專門介紹設計安全工作的部分。汽車年度財務報告通常包含有關駕駛員和乘客安全的章節，包括有關集中式和分散式質量和安全委員會的資訊。在財務報告中詳細說明設計安全計劃將表明該組織正在將客戶安全與企業財務成果聯繫起來，而不是簡單地在行銷材料中採用一個流行術語。

2. **向董事會提供定期報告。**首席資訊安全官(CISO)向公司董事會提交的報告通常包括有關當前和計劃的安全計劃、威脅、可疑和已確認的安全事件等資訊，以及以公司安全態勢和健康狀況為中心的最新資訊。除了接收有關企業安全態勢的資訊外，董事會還應要求有關產品安全及其對客戶安全影響的資訊。董事會不應僅依靠 CISO，而應主要依靠公司管理階層的其他成員來降低客戶風險。

3. **授權設計安全主管。**技術團隊擁有「主管認可」的組織，與業務領導者使用標準業務流程親自管理客戶安全改善流程的組織之間，存在顯著差異。「主管認可」一詞意味著必須有人來推銷客戶安全計畫的理念，而不是將其作為頂級商業目標。該主管必須有權影響產品投資，以實現客戶安全成果。

4. **創造有意義的內部激勵機制。**在留意不要創造反常激勵的同時，調整獎勵制度來提高客戶安全性，以配對其他有價值的行為和結果。從設計安全主管到產品管理、軟件開發、支援、銷售、法律和其他組織，將客戶安全激勵機制融入招聘、晉升、薪資、獎金、股票期權和業務營運的其他常見流程。例如，在製定晉升軟件開發人員的標準時，應將提高產品安全性與正常運作時間、效能和功能改進等其他標準一併考慮。

5. **創建設計安全委員會。**在某些產業中，機構通常會建立一個中央質量委員會，並在關鍵部門或業務單位中設立質量代表。透過包括集中式和分散式成員，這些小組在接收來自組織深處的遙測資訊的同時，還能根據高層目標提高質量。同樣，設計安全委員會將根據整個組織的設計安全目標提高安全性。

6. **創建並發展客戶委員會。**許多軟件製造商都有由來自不同地區、行業和規模的客戶組成的客戶委員會。這些委員會可以提供大量有關客戶在部署公司產品方面取得的成功和面臨的挑戰的資訊。在制定客戶委員會議程時，即使客戶安全問題目前還不是參與者目前最關心的問題，也應將其作為專門的主題。考慮客戶委員會的報告內容，以及如何挖掘參與者對產品部署安全性的見解。例如，客戶委員會是偏重行銷和銷售目的，還是產品管理？設計安全主管應協助引導這些客戶互動，並將其與本文中的其他要素（例如實地研究）連結起來。

設計安全策略

安全軟件開發框架 (SSDF)，也稱為美國國家標準與技術研究院 (NIST) SP 800-218，是一套核心的高級安全軟件開發實踐，可整合到軟件開發生命週期(SDLC)每個階段。遵循這些做法可以幫助軟件生產商更有效地發現和消除已發布軟件中的漏洞，減輕利用漏洞可能造成的潛在影響，並解決漏洞的根本原因以防止將來再次發生。

編寫機構鼓勵使用設計安全策略，包括參考SSDF實踐的原則。軟件製造商應制定書面路線圖，以便在其產品組合中採用更安全的設計軟件開發實踐。以下是路線圖最佳實踐的非詳盡說明性清單：

- **記憶體安全編程語言 (SSDF PW.6.1)**。盡可能優先使用記憶體安全語言。編寫機構承認，特定於記憶體的緩解措施可能是有助於遺留代碼庫的短期策略。例如 C/C++ 語言改進、硬件緩解、地址空間佈局隨機化(ASLR)、控制流完整性(CFI)和模糊處理。儘管如此，越來越多的人認為採用記憶體安全程式語言可以消除此類缺陷，軟件製造商應該探索採用它們的方法。現代記憶體安全語言的一些例子包括 C#、Rust、Ruby、Java、Go 和 Swift。請閱讀 NSA 的記憶體安全 資訊表，了解更多資訊。
- **安全硬件基礎**。整合可實現細粒度記憶體保護的架構功能，例如可擴展傳統硬件指令集架構 (ISA) 的功能硬件增強 RISC 指令 (CHERI) 所描述的功能，以及可信任平台模組和硬件安全模組等其他功能。欲了解更多資訊，請瀏覽劍橋大學的 CHERI 網頁。
- **安全軟件組件(SSDF PW 4.1)**。從經過驗證的商業、開源和其他第三方開發人員處取得並維護安全良好的軟件組件（例如軟件庫、模組、中間件、框架），以確保消費軟件產品的強大安全性。
- **網絡模板框架(SSDF PW.5.1)**。使用可自動轉義用戶輸入的網絡模板框架，以避免跨站腳本等網絡攻擊。
- **參數化查詢（SDF PW 5.1）**。使用參數化查詢而不是在查詢中包含用戶輸入，以避免 SQL 注入攻擊。
- **靜態和動態應用程式安全測試(SAST/DAST)**（SSDF PW.7.2、PW.8.2）。使用這些工具分析產品原始碼和應用程式行為，以檢測容易出錯的做法。這些工具涵蓋的問題範圍從記憶體管理不當到資料庫查詢構造容易出錯（例如，未轉義的用戶輸入導致 SQL 注入）。SAST和 DAST 工具可以納入到開發流程中，並作為軟件開發的一部分自動運作。SAST和DAST應作為單元測試和集成測試等其他類型測試的補充，以確保產品符合預期的安全要求。當發現問題時，製造商應進行根本原因分析，以系統地解決漏洞。

- **代碼審查**（SSDF PW.7.1、PW.7.2）。努力確保提交到產品中的代碼經過質量控制技術，例如其他開發人員的同儕評審或「錯誤植入」。
- **軟件物料清單 (SBOM)** (SDF PS.3.2、PW.4.1)。納入 SBOM[4] 的創建，以提供產品中的軟件集的可見性。
- **漏洞披露計畫**(SSDF RV.1.3)。建立漏洞披露計劃，允許安全研究人員報告漏洞並獲得法律安全港。作為其中的一部分，供應商應建立流程來確定已發現漏洞的根本原因。此類流程應包括確定採用本文件中的任何設計安全實踐（或其他類似實踐）是否可以防止漏洞的引入。
- **CVE 完整性**。確保發布的 CVE 包含根本原因或通用缺陷列表 (CWE)，以便能夠對軟件安全設計缺陷進行在全行業範圍分析。雖然確保每個 CVE 的正確和完整可能需要額外的時間，但它可以讓不同的實體發現有利於所有製造商和客戶的行業趨勢。有關管理漏洞的詳情，請參閱 CISA 的利益相關者特定漏洞分類 (SSVC) 指南。
- **縱深防禦**。設計基礎設施，確保單一安全控制的破壞不會導致整個系統的破壞。例如，確保嚴格規定用戶權限並採用存取控制清單，就可以減少帳戶遭受破壞的影響。此外，軟件沙箱技術可以隔離漏洞，以限制對整個應用程式造成的破壞。
- **滿足網絡安全性能目標 (CPG)**。設計符合基本安全實踐的產品。CISA 的網絡安全性能目標概述了機構應實施的基本和基準網絡安全措施。此外，如需了解更多增強機構態勢的方法，請參閱英國的網絡評估架構，該框架與 CISA 的 CPG 具有相似之處。如果製造商未能滿足 CPG（例如不要求所有員工都具備防網絡釣魚 MFA），那麼他們就不能被視為提供設計安全的產品。

編寫機構認識到這些變化是機構態勢的重大轉變。因此，應根據定制的威脅建模、關鍵性、複雜性和業務影響來確定引入它們的優先順序。可以針對新軟件引入這些實踐，並逐步擴展以涵蓋其他用例和產品。在某些情況下，某些產品的關鍵性和風險態勢可能需要加快採用這些實踐的進度。在其他情況下，可以將這些實踐引入遺留代碼庫並隨著時間的推移進行修復。

[4] 一些編寫機構正在探索替代方法來獲得軟件供應鏈的安全保證。

預設安全策略

除了採用設計安全開發實踐外，編寫機構還建議軟件製造商在其產品中優先考慮預設安全的配置。這些製造商應該努力更新產品，以便在產品更新時符合這些實踐。例如：

- **消除預設密碼。**產品不應帶有普遍共用的預設密碼。為消除預設密碼，編寫機構建議產品要求管理員在安裝和配置期間設置一個強密碼，或為產品的每台設備提供獨特的強度密碼。

- **對特權用戶強制執行多因素身份驗證(MFA)。**我們觀察到許多企業部署是由未使用MFA保護的帳戶的管理員管理的。鑑於管理員是高價值目標，產品應該讓 MFA 選擇退出而不是選擇加入。此外，系統應定期提示管理員註冊MFA，直到他們在其帳戶上成功啟用它。荷蘭的NCSC有與 CISA 類似的指導，請查閱他們的成熟認證資訊單張了解更多資訊。

- **單點登錄(SSO)。** IT 應用程式應通過現代開放標準實施單點登錄技術。這方面的示例包括安全斷言標記式語言 (SAML) 或 OpenID連接(OIDC)。此功能應預設提供，無需額外費用。

- **安全日誌**為客戶提供高質量的審計日誌，不收取額外費用。審計日誌對於檢測和升級潛在的安全事件至關重要。它們在調查疑似或已確認的安全事件期間亦甚為重要。考慮最佳做法，例如將安全資訊和事件管理系統與使用協調世界時(UTC)、標準時區格式和強大的文件技術的應用程式編程接口 (API)更易於整合。

- **軟件授權配置文件。**軟件供應商應提供有關授權配置文件角色及其指定使用情況的建議。製造商應包括一個明顯的警告，通知客戶如果他們偏離了建議的配置文件授權，就會增加風險。例如：醫生可以查看所有患者記錄，但醫療調度員對安排預約所需的某些資訊的存取權限有限。

- **前瞻性安全優於後向兼容性。**向後兼容的遺留功能往往包含在產品中，並且經常在產品中啟用，儘管這會給產品安全帶來風險。將安全性置於向後兼容性之上，使安全團隊能夠刪除不安全的功能，即使這意味著會導致重大更改。

- **跟踪並縮減「加固指南」的大小。**縮減為產品製作的「加固指南」的大小，並努力確保隨著軟件新版本的發布，尺寸會越來越小。將「加固指南」的組件整合為產品的預設配置。編寫機構認識到，縮短加固指南是與現有客戶持續合作的結果，包括許多產品團隊的努力，包括用戶體驗 (UX)。

- **考慮安全設置對用戶體驗的影響。**每個新設置都會增加最終用戶的認知負擔，應該結合所帶來的商業利益進行評估。理想情況下，一個設置不應該存在； 相反，最安全的設置應該預設集成到產品中。當配置是必要的時候，預設選項應能夠廣泛地對抗常見威脅。

編寫機構承認這些變化可能會對軟件的使用方式產生操作影響。因此，客戶的意見對於平衡操作和安全考慮至關重要。我們相信制定書面路線圖和行政支持，將這些想法優先納入組織最關鍵的產品中，是轉向安全軟件開發實踐的第一步。雖然客戶的意見很重要，但編寫機構觀察到一些客戶不願或不能採用改進標準（通常是網絡協議）的重要案例。對於製造商來說，重要的是要為客戶創造有意義的激勵措施，讓他們保持最新，並不允許他們無限期地存在漏洞。

加固與鬆散指南

加固指南的產生可能是由於缺乏從開發之初就嵌入到產品架構中的產品安全控制。因此，加固指南也可以成為對手查明和利用不安全功能的路線圖。許多組織通常不知道強化指南，因此他們的設備配置設置處於不安全的狀態。一種被稱為鬆動指南的倒置模型應該取代這種加固指南，並解釋用戶應該進行哪些更改，同時列出由此產生的安全風險。這些指南應該由安全從業人員編寫，他們可以用清晰的語言解釋其中的利弊，以增加正確應用它們的機會。

編寫機構建議軟件製造商通過提供「鬆散指南」轉向預設安全方法，而不是開發列出保護產品方法的強化指南。這些指南以通俗易懂的語言解釋決策的商業風險，並可以提高組織對惡意網絡入侵風險的認識。安全權衡應由客戶的高級管理人員決定，平衡安全與其他業務需求。

給客戶的建議

編寫機構建議組織讓他們的供應軟件製造商對其產品的安全結果負責。作為其中的一部分，編寫機構建議組織高管將購買「設計安全」和「預設安全」產品的重要性放在首位。這可以通過制定政策要求 IT 部門在購買製造商軟件之前評估其安全性，以及授權 IT 部門在必要時推回來體現。應授權 IT 部門製定採購標準，強調「設計安全」和「預設安全」實踐（本文件中概述的那些以及組織製定的其他實踐）的重要性。此外，在採購決策中執行這些標準時，IT 部門應該得到執行管理層的支持。接受與特定技術產品相關風險的組織決策應正式記錄在案，由高級業務主管批准，並定期提交給董事會。

支持組織安全態勢的關鍵企業 IT 服務，例如企業網絡、企業身份和存取管理以及安全運營和響應能力，應被視為關鍵業務功能，對其提供的資金與其對組織任務成功的重要性保持一致。組織應制定計劃，升級這些功能，以採用「設計安全」和「預設安全」實踐的製造商。

在可能的情況下，組織應努力與他們的主要 IT 供應商建立戰略夥伴關係。這種關係包括組織多個級別的信任，並提供解決問題和確定共同優先事項的工具。安全應該是這種關係的一個關鍵要素，組織應該努力在關係的正式（例如，合同或供應商協議）和非正式方面加強「設計安全」和「預設安全」實踐的重要性。組織應該期望其技術供應商對其內部控制狀況以及採用「設計安全」和「預設安全」實踐的路線圖保持透明。

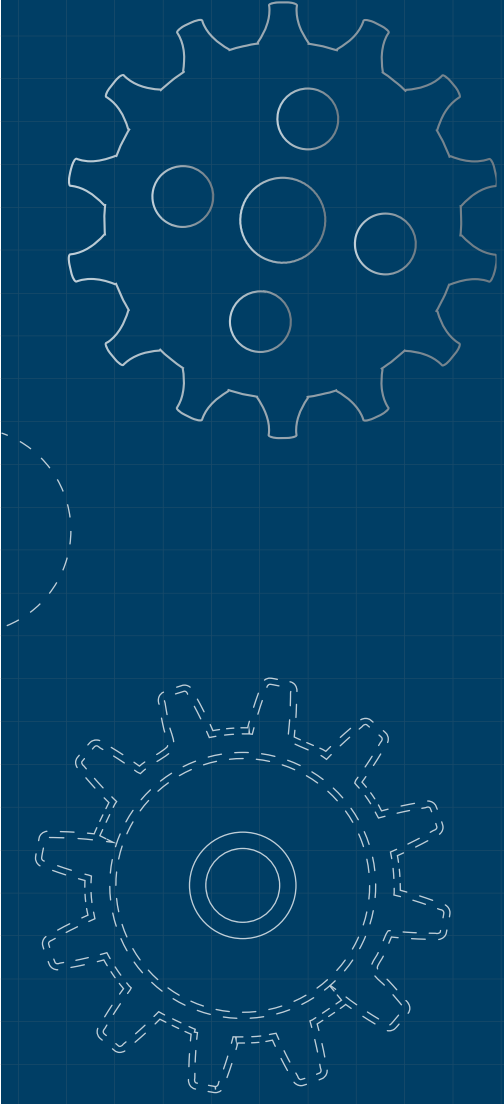
除了將「預設安全」作為組織內的優先事項外，IT 領導者還應與業內同行合作，了解哪些產品和服務最能體現這些設計原則。這些領導者應協調他們的請求，以幫助製造商安排他們即將推出的安全計劃的優先次序。通過合作，客戶可以幫助向製造商提供有意義的意見，並為他們創造優先考慮安全性的激勵措施。

在利用雲端系統時，組織應確保他們了解與其技術供應商的責任共擔模式。也就是說，組織應該清楚供應商的安全責任，而不僅僅是客戶的責任。

組織應該優先考慮那些對其安全狀態、內部控制和在責任共擔模式下履行自己義務的能力透明的供應商。

免責聲明

本報告中的資訊按「原樣」提供，僅供參考。CISA 和編寫機構不認可任何商業產品或服務，包括任何分析對象。任何通過服務標誌、商標、製造商或其他方式對特定商業實體或商業產品、流程或服務的提及，並不構成或暗示 CISA 和編寫機構的背書、推薦或偏袒。本文件是 CISA 的聯合倡議，並不自動作為監管文件。



資源

CISA

- 軟件組件清單 (SBOM) 指南
- CISA 跨行業網絡安全績效目標
- 技術互通性指南
- CISA和 NIST的防禦軟件供應鏈
- 不安全技術的代價及我們能夠採取的措施 | CISA
- 停止推卸網絡安全責任：為什麼公司必須將安全納入科技產品中 (foreignaffairs.com)
- CISA利益相關者特定漏洞分類 (SSVC) 指南
- CISA的防釣魚多重身份驗證資訊單張
- 給小企業的網絡安全指南 | CISA

NSA

- NSA的內存安全網絡安全資訊表
- NSA的ESF 確保軟件供應鏈安全：供應商的最佳做法

FBI

- 理解和應對 SolarWinds 供應鏈攻擊：聯邦的觀點
- 網絡威脅–應對和報告
- FBI 的網絡安全策略

國家標準與技術研究所 (NIST)

- NIST 的數碼身份指南
- NIST 的網絡安全框架
- NIST 的安全軟件開發框架 (SSDF)

澳洲網絡安全中心 (ACSC)

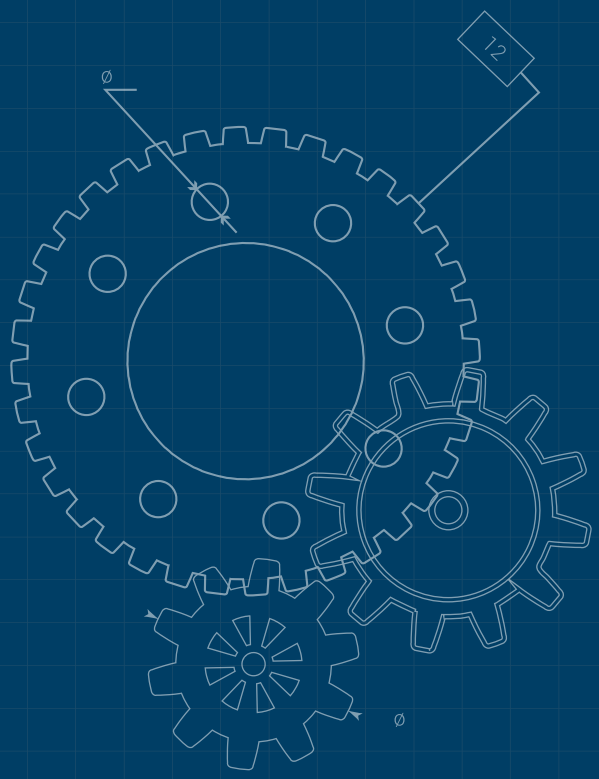
- ACSC 的物聯網製造商守則指南

英國國家網絡安全中心 (UK)

- 英國的網絡評估框架
- 英國 NCSC 的安全開發與部署指南
- 英國 NCSC 的漏洞管理指南
- 英國 NCSC 的漏洞披露工具包
- 劍橋大學的 CHERI
- 再見，感謝所有的位元組–NCSC.GOV.UK

加拿大網絡安全中心 (CCS)

- CCCS 的防範軟件供應鏈攻擊指南
- 網絡供應鏈：風險評估方法
- 加拿大網絡安全中心提供的CONTI勒索軟件指南 (CCS)



德國聯邦資訊安全辦公室(BSI)

» BSI Grundschutz綱要（模組CON.8）
» 國際標準IEC 62443第4-1部分
» 2022年德國IT安全狀況報告
» BSI網站應用安全的最佳實踐

荷蘭國家網絡安全中心

» NCSC-NL成熟身份驗證資訊單張

日本國家網絡安全事故準備與戰略中心 (NISC)

» 日本國家網絡安全戰略

日本經濟產業省 (METI)

» 軟件管理軟件物料清單 (SBOM) 介紹指引
» 有關使用 OSS 和確保其安全性的管理方法的用例範例集合

新加坡網絡安全局

» 安全 API 開發技術諮詢
» CSA SingCERT 漏洞披露政策
» CSA SingCERT 事故響應清單
» CSA SingCERT 事故響應手冊
» CSA 設計安全架構
» CSA 設計安全框架清單
» CSA 網絡威脅建模指南
» CSA 網絡安全標籤計劃

其他

» 複雜系統是如何失敗的
» 複雜系統故障的新觀點

參考文獻

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran on Quality by Design by J.M. Juran, 1992.