TLP:CLEAR

改变网络安全风险平衡：设计安全和默认安全的原则和方法

发布时间： 2023年4月13日

美国网络安全和基础设施安全局

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

目录

概述：易受攻击的设计

技术已经融入到人们日常生活的几乎所有方面。面向互联网的系统连接到直接影响我们经济繁荣、生计甚至健康的关键系统，其范围包括个人身份管理到医疗保健等各方面。仅举一个例子，网络漏洞已在全球范围内导致医院取消手术并转移患者护理。关键系统中的不安全技术和漏洞可能会招致恶意网络入侵，从而导致严重的潜在安全[1]风险。

技术制造商需要将设计安全和默认安全作为产品设计和开发流程的重点，这在现在比以往任何时候都更重要。一些供应商在软件保障方面取得了巨大的进展，推动行业向前发展，而有些供应商则落后于此。编写机构强烈鼓励每个技术制造商以客户无需不断对其系统进行监控、例行更新和损坏控制的方式来构建他们的产品，以减轻网络入侵的影响。鼓励制造商承担起改善其客户安全成果的责任。过去，技术制造商一直依赖于修复客户部署产品后所发现的漏洞，并要求客户自费应用这些补丁。只有采纳“设计安全”实践，我们才能打破创建并应用修复补丁的恶性循环。

为了实现这种高标准的软件安全，编写机构鼓励制造商优先考虑将产品安全性的融入作为功能和上市速度的关键先决条件。随着时间的推移，工程设计团队将能够建立一种新的稳态节奏，其中安全性真正融入设计之中，并且维护工作量更少。

与这一观点不谋而合的是，欧盟在《网络弹性法案》中强调了产品安全的重要性，强调制造商应在产品的整个生命周期实施安全措施，以防止制造商将易受攻击的产品引入市场。

为了创造一个技术和相关产品对客户来说更安全的未来，编写机构敦促制造商改进他们的设计和开发计划，只允许将设计安全和默认安全的产品运送给客户。设计安全的产品是指客户安全不只是技术功能，而且是核心业务目标的产品。设计安全的产品在开始开发之前就以该目标为出发点。默认安全的产品是那些“开箱即可安全使用”的产品，几乎或完全不需要更改配置，并且无需额外费用即可拥有安全功能。

若将这两个原则相结合，那么保持安全的大部分责任就被转移给了制造商，并降低了客户成为因配置错误、补丁速度不够快或许多其他常见问题导致的安全事件受害者的可能性。

美国网络安全和基础设施安全局 (CISA) 、美国国家安全局 (NSA) 、美国联邦调查局 (FBI) 和以下国际合作伙伴[2] 在本指南中提供了建议，作为技术制造商确保其产品安全的路线图：

- 澳大利亚网络安全中心 (ACSC)
- 加拿大网络安全中心 (CCCS)
- 英国国家网络安全中心 (NCSC-UK)

[1] 编写机构认识到“安全”一词根据其上下文具有多种含义。在本指南中，“安全”是指提高技术安全标准以保护客户免受恶意网络活动的侵害。
[2] 以下称为“编写机构”。

- 德国联邦信息安全办公室 (BSI)
- 荷兰国家网络安全中心 (NCSC-NL)
- 新西兰计算机应急响应小组(CERT NZ) 和新西兰国家网络安全中心 (NCSC-NZ)。

编写机构承认许多私营部门的合作伙伴在推进设计安全和默认安全方面所做的贡献。本文档旨在推动有关关键优先事项、投资和决策的国际对话，以实现技术在设计上和默认情况下安全、可靠和有弹性的未来。为此，编写机构向有关各方征求对本文档的反馈，并打算召开一系列反馈会，以进一步完善、明确和推进我们的指南，从而实现我们的共同目标。

有关产品安全重要性的更多信息，请参阅 CISA 的文章 -- 《不安全技术的代价以及我们可以采取的措施》。

设计安全

“设计安全”意味着技术产品的构建方式可以合理地防止恶意网络参与者成功访问设备、数据和连接的基础设施。软件制造商应开展风险评估，以识别和列举关键系统所面临的普遍网络威胁，然后在产品蓝图中包含保护措施，以应对不断变化的网络威胁形势。

我们还建议采用安全信息技术 (IT) 开发实践和多层防御（称为纵深防御），以防止敌对活动危害系统或未经授权访问敏感数据。编写机构建议制造商在产品开发阶段使用定制的威胁模型来解决对系统的所有潜在威胁，并考虑每个系统的部署过程。

编写机构敦促制造商对其产品和平台采取全面的安全措施。设计安全的开发需要软件制造商在产品设计和开发过程的每一层都投入大量资源，而这些资源不能在以后“附加”。它要求制造商高层业务主管发挥强有力的领导作用，将安全作为业务优先事项，而不仅仅是一项技术功能。业务领导人员和技术团队之间的这种协作要从设计和开发的早期阶段一直延伸到客户部署和维护阶段。我们鼓励制造商做出艰难的权衡和投资，包括那些对客户“不可见”的权衡和投资，例如迁移到消除普遍存在的漏洞的编程语言。他们应该优先考虑保护客户的功能、机制并实施保护客户的工具，而不是那些看起来很有吸引力但会扩大攻击面的产品功能。

没有任何单一的解决方案可以结束由恶意网络参与者利用技术漏洞所带来的持续威胁，而且“设计安全”的产品也将继续受到漏洞的影响；但是，大量的漏洞是由一部分相对较小的根本原因造成的。制造商应制定书面路线图，以使其现有产品组合与更多“设计安全”实践保持一致，确保仅在特殊情况下才偏离这种实践。

编写机构承认，对客户安全成果负责并确保这种级别的客户安全可能会增加开发成本。但是，在开发新技术产品和维护现有产品的同时，向“设计安全”实践投资可以显著改善客户的安全状况，并降低受到威胁的可能性。“设计安全”原则不仅可以增强客户的安全状况和开发人员的品牌声誉，而且从长远来看还可以降低制造商的维护和修补成本。

下方列出的“对软件制造商的建议”部分提供了建议的产品开发实践和政策清单，以供制

造商考虑。

默认安全

“默认安全”意味着产品开箱即可抵御普遍存在的攻击技术，无需额外付费。这些产品可以抵御最普遍的威胁和漏洞，而最终用户无需采取额外的措施来保障其安全。“默认安全”的产品旨在让客户敏锐地意识到，当他们偏离安全的默认设置时，除非他们实施额外的补偿控制措施，否则他们会增加受攻击的可能性。

- 安全配置应该是默认基线。“默认安全”的产品会自动启用最重要的安全控制措施，以保护企业免受恶意网络参与者的攻击，并且可以在无需额外费用的情况下使用和进一步配置安全控制措施。
- 安全配置的复杂性不应是客户的问题。组织的 IT 员工经常负担过重的安全和运营责任，从而导致只有有限的时间来理解和处理安全隐患和实施缓解措施，而这些是实现稳健的网络安全态势所需的工作。通过优化安全产品配置 —— 确保“默认路径”的安全 —— 制造商可确保他们的产品按照“默认安全”标准安全地制造、分销和使用，从而帮助他们的客户。

“默认安全”产品的制造商不会为实施额外的安全配置收取额外费用。相反，他们将这些安全配置包含在基础产品中，就像所有新车都包含安全带一样。安全不是奢侈的选择，而是更接近每个客户应该期望的标准，无需谈判或支付更多费用。

对软件制造商的建议

这份联合指南为制造商制定书面路线图以实施和确保 IT 安全提供了建议。编写机构建议软件制造商实施以下部分中概述的策略，以通过设计安全和默认安全的原则来对客户安全成果负责。

软件产品安全原则

我们鼓励技术制造商采取优先考虑软件安全的战略重点。编写机构制定了以下三个核心原则，以指导软件制造商在开发、配置和交付其产品之前将软件安全构建到其设计过程中。

1. 安全的责任不应该只落在客户身上。软件制造商应对客户购买其产品的安全成果负责，并相应地改进其产品。
2. 奉行完全透明和问责制。软件制造商应该提供安全可靠的产品，凭借自己的这一能力在制造商社区中与众不同，并对此感到自豪。这可包括分享他们从客户部署中学到的信息，例如默认采用强大的身份验证机制。这也包括坚定承诺确保漏洞警报和相关的常见漏洞和曝光 (CVE) 记录完整、准确。然而，要警惕将CVE视为负面指标的诱惑，因为这些数字也是健康的代码分析和测试社区的标志。
3. 建立组织结构和领导力来实现这些目标。虽然技术主题方面的专业知识对于产品安

全至关重要，但高层管理人员是在组织中实施变革的主要决策者。软件制造商的高层管理人员承诺将安全优先作为产品开发的关键要素，这需要与组织的客户建立合作伙伴关系，以了解以下内容：

a. 产品部署场景指南以及定制的威胁模型
b. 安全控制措施的拟议实施，以符合默认安全原则
c. 根据公司规模量身定制的资源分配策略以及用设计安全实践取代遗留开发实践的能力
d. 需保持开放的沟通渠道以获取有关产品安全问题的内部和外部反馈（例如，员工和客户反馈）。应在内部讨论会（例如全员大会或非正式会议）以及外部产品营销和客户参与中强调软件安全
e. 衡量客户部署中的有效性。高层管理人员希望了解，通过减缓安全补丁的速度、减少配置错误和最小化攻击面，对设计安全和默认安全的投资在哪些方面帮助了客户。

为了实现这三个原则，制造商应该考虑几种运营策略来改进他们的开发流程。

与公司高层领导召开例行会议，以便在组织内推动对“设计安全”和“默认安全”的重视。应制定政策和程序来奖励开发遵守这些原则的产品的生产团队，这可以包括对实施出色的软件安全实践提供奖励，或晋升阶梯和晋升标准方面的激励措施。

围绕软件安全对业务成功的重要性开展工作。例如，考虑指定一名“软件安全负责人”或一支“软件安全团队”来专门负责维护业务和 IT 实践，以直接将软件安全标准与制造商责任联系起来。制造商应确保他们的产品拥有稳健、独立的产品安全评估和评价程序。

在开发过程中使用定制的威胁模型来优先考虑最关键和影响最大的产品。威胁模型需考虑产品的特定用例，并使开发团队能够强化产品。最后，高层领导人员应该让团队负责交付安全的产品，将其作为产品卓越性和质量的关键要素。

设计安全的策略

安全软件开发框架(SSDF)（也称为美国国家标准与技术研究院 (NIST) SP 800-218）是一套核心的高级安全软件开发实践，可以集成到软件开发生命周期（SDLC）的每个阶段。遵循这些实践可以帮助软件生产商更有效地发现和消除已发布软件中的漏洞，减轻漏洞受攻击的潜在影响，并解决漏洞存在的根本原因以防止未来再次发生。

编写机构鼓励使用设计安全策略，包括参考 SSDF 实践的原则。软件制造商应制定书面路线图，以在其产品组合中采用更多“设计安全”软件开发实践。以下是一些举例的路线图最佳实践，列表并不详尽：

- 内存安全编程语言(SSDF PW.6.1)：尽可能优先使用内存安全语言。编写机构承认其他内存特定的缓解措施，如地址空间布局随机化 (ASLR)、控制流完整性 (CFI) 和模糊

测试 (fuzzing) 对遗留代码库有帮助，但不足以被视为设计安全，因为这些措施不能充分防止被攻击。现代内存安全语言的一些示例包括 C#、Rust、Ruby、Java、Go 和 Swift。阅读 NSA 的内存安全信息单以了解更多信息。

- 安全硬件基础：整合能够实现细粒度内存保护的架构功能，例如可扩展传统硬件指令集架构 (ISA) 的功能硬件增强的 RISC 指令 (CHERI) 所描述的架构功能。如需了解更多信息，请访问剑桥大学的 CHERI网页。
- 安全软件组件 (SSDF PW 4.1)：从经过验证的商业、开源和其他第三方开发人员处获取和维护安全可靠的软件组件（例如，软件库、模块、中间件、框架），以确保消费者软件产品的稳健安全性。
- Web 模板框架(SSDF PW.5.1)：使用实现了自动转义用户输入的 Web 模板框架，以避免 Web 攻击，如跨站点脚本攻击。
- 参数化查询(SSDF PW 5.1)：使用参数化查询，而不是在查询中包含用户输入，以避免 SQL 注入攻击。
- 静态和动态应用程序安全测试(SAST/DAST)(SSDF PW.7.2、PW.8.2)：使用这些工具来分析产品源代码和应用程序行为，以检测容易出错的做法。这些工具涵盖了从内存管理不当到容易出错的数据库查询构造（例如，未转义的用户输入导致 SQL 注入）的问题。SAST 和 DAST 工具可以整合到开发过程中，并作为软件开发的一部分自动运行。SAST 和 DAST 应该补充其他类型的测试，例如单元测试和集成测试，以确保产品符合预期的安全要求。发现问题后，制造商应进行根本原因分析，以系统地解决漏洞。
- 代码审查(SSDF PW.7.1、PW.7.2)：努力确保提交到产品中的代码经过其他开发人员的同行审查，以确保更高的质量。
- 软件物料清单 (SBOM) (SSDF PS.3.2, PW.4.1)：纳入 SBOM[3] 的创建，以提供对进入产品的软件集的可见性。
- 漏洞披露计划(SSDF RV.1.3)：建立漏洞披露计划，允许安全研究人员报告漏洞并在此过程中获得法律安全保障。作为其中的一部分，供应商应建立流程来确定已发现漏洞的根本原因。此类流程应包括确定采用本文档中的任何“设计安全”实践（或其他类似实践）是否可以防止引入漏洞。
- 常见漏洞和曝光（CVE）的完整性：确保已发布的 CVE 包括根本原因或常见弱点枚举 (CWE)，以便在整个行业范围内分析软件安全根本原因。虽然确保每个 CVE 都正确、完整可能需要额外的时间，但它允许不同的实体发现有利于所有制造商和客户的行业趋势。有关管理漏洞的更多信息，请参阅CISA专门针对利益相关者的漏洞分类（SVCC）指南。
- 纵深防御：设计基础设施，使单个安全控制受损不会导致整个系统受损。例如，确

[3] 一些编写机构正在探索替代方法来获得软件供应链方面的安全保证。

保严格规定用户权限并使用访问控制列表，这可以减少被盗账户的影响。此外，软件沙箱技术可以将漏洞隔离，以限制整个应用程序受损。

- 满足网络性能目标(CPG)：设计满足基本安全实践的产品。CISA 的网络安全性能目标概述了组织应该实施的基本的基准网络安全措施。此外，有关加强组织态势的更多方法，请参阅英国网络评估框架，该框架与 CISA 的 CPG 有相似之处。

编写机构认识到这些变化是组织态势的重大转变。因此，应根据关键性、复杂性和对业务的影响来对引入这些变化进行优先排序。可以为新软件引入这些实践，并逐步扩展以涵盖其他用例和产品。在某些情况下，某种产品的关键性和风险态势可能值得加快采用这些实践。在其他情况下，可以将这些实践引入遗留代码库中并随着时间的推移进行纠正。

默认安全的策略

除了采用“设计安全”的开发实践外，编写机构还建议软件制造商在其产品中优先考虑“默认安全”的配置。他们应该努力在产品更新时遵循这些实践。例如：

- 消除默认密码：产品不应带有普遍共享的默认密码。为消除默认密码，编写机构建议产品要求管理员在安装和配置期间设置强密码。
    - o 针对特权用户强制执行多重身份验证 (MFA) 。 我们观察到，许多企业是由未使用 MFA 保护其账户的管理员管理部署的。 鉴于管理员是高价值目标，产品应该将 MFA 设为默认启用，而非可选启用。此外，系统应定期提示管理员注册 MFA，直到他们在其账户上成功启用。荷兰国家网络安全中心（NCSC）有与 CISA 类似的指南，如需了解更多信息，请访问他们的成熟身份认证资料单。
- 单点登录(SSO)：IT 应用程序应通过现代开放标准实施单点登录技术。示例包括安全断言标记语言 (SAML) 或 OpenID Connect (OIDC)。此功能应默认提供，无需额外费用。
- 安全日志记录：为客户提供高质量的审计日志，无需额外费用。审计日志对于检测潜在的安全事件并对其进行升级处理至关重要。在调查疑似或已确认的安全事件期间，它们也至关重要。考虑最佳实践，例如提供与安全信息和事件管理 (SIEM) 系统的轻松集成，这些系统具有使用协调世界时 (UTC)、标准时区格式和强大文档技术的应用程序编程接口 (API) 访问。
- 软件授权配置文件：软件供应商应提供有关授权配置文件的作用及其指定用例的建议。制造商应包括一个明显的警告，如果客户不使用推荐的授权配置文件，则通知客户会存在更高的风险。例如：医生可以查看所有患者记录，但医疗调度员对安排预约所需的地址信息拥有有限的访问权限。
- 优先考虑前瞻安全性，而非向后兼容性：尽管向后兼容性会对产品安全造成风险，但产品中仍然经常包含并经常启用向后兼容的遗留功能。优先考虑安全性而非向后

兼容性，赋予安全团队权力来移除不安全的功能，即使这意味着会导致重大更改。

- 跟踪并缩小“加固指南”的大小：缩小为产品制作的“加固指南”的大小，并努力确保随着软件新版本的发布，“加固指南”的大小会随着时间的推移而缩小。将“加固指南”的组件整合为产品的默认配置。编写机构认识到，缩短的加固指南是与现有客户持续合作的结果，需要包括用户体验 (UX)在内的许多产品团队的努力。
- 考虑安全设置对用户体验的影响：每个新设置都会增加最终用户的认知负担，应结合它带来的商业利益进行评估。理想情况下，不应该存在设置；相反，最安全的设置应该默认整合到产品中。当需要配置时，默认选项应该有广泛的安全性以抵御常见威胁。

编写机构承认，这些变化可能会对软件的使用方式产生操作上的影响。因此，为了权衡操作和安全考量，客户的意见至关重要。编写机构认为，制定书面路线图以及优先考虑将这些想法融入组织最关键的产品中并受到高层管理人员的支持，是转向安全软件开发实践的第一步。虽然客户的意见很重要，但编写机构观察到客户不愿意或不能采用改进标准（通常是网络协议）的重要案例。对于制造商来说，重要的是要为客户创造有意义的激励措施，来让他们保持最新状态，而不是让他们无限期地保持易受攻击的状态。

加固指南与宽松指南

加固指南可能源于产品安全控制从开发开始就未嵌入产品架构的情况。因此，加固指南也可以成为对手确定和利用不安全功能的路线图。许多组织通常不知道加固指南，因此他们将其设备配置设置置于不安全的态势。应该由一种倒置模型（称为宽松指南）来取代这种加固指南，并向用户解释他们应该进行哪些更改，同时列出由此产生的安全风险。

编写机构建议软件制造商通过提供宽松指南来转向默认安全的方法，而不是开发加固指南来列出保护产品的方法。这些指南以通俗易懂的语言解释决策的业务风险，并可以提高组织对恶意网络入侵风险的意识。安全权衡应由客户的高级管理人员决定，以便在安全与其他业务需求之间取得平衡。

对客户的建议

编写机构建议组织让他们的供应技术制造商对其产品的安全结果负责。作为其中的一部分，编写机构建议组织高层管理人员优先考虑购买设计安全和默认安全产品的重要性。这可以通过制定政策来实现，要求 IT 部门在购买制造商软件之前评估其安全性，以及授权 IT 部门在必要时予以反对。应授权 IT 部门制定采购标准，强调设计安全和默认安全实践（本文档中概述的那些实践以及组织制定的其他实践）的重要性。此外，在采购决策中执行这些标准时，IT 部门应该得到高层管理人员的支持。组织在决定接受与特定技术产品相关的风险时，应将这些决定正式记录在案，由高级业务管理人员批准，并定期提交给董事会。

支持组织安全态势的关键企业 IT 服务，例如企业网络、企业身份和访问管理以及安全运作和响应能力，应被视为关键的业务功能，因此这些服务的资金应与其对组织任务成功的重

要性保持一致。组织应制定升级这些功能的计划，以便利用采用设计安全和默认安全实践的制造商。

在可能的情况下，组织应努力与其主要 IT 供应商建立战略合作伙伴关系。这种关系包括组织中多个级别的信任，并提供解决问题和确定共同优先事项的工具。安全应该是这种关系的一个关键要素，组织应该努力在这种关系的正式（例如，合同或供应商协议）和非正式方面加强设计安全和默认安全实践的重要性。组织应该期望其技术供应商对其内部控制态势以及采用“设计安全”和“默认安全”实践的路线图保持透明。

除了将默认安全作为组织内的优先事项外，IT 领导人员还应与其行业同行合作，以了解哪些产品和服务最能体现这些设计原则。这些领导人员应该协调他们的请求，以帮助制造商优先考虑他们即将推出的安全性举措。通过合作，客户可以帮助向制造商提供有意义的反馈意见，并创造激励措施，使他们优先考虑安全性。

在利用云系统时，组织应确保他们了解与其技术供应商的责任共担模型。即，组织应该清楚供应商的安全责任，而不仅仅是客户的责任。组织应优先考虑对其安全态势、内部控制以及履行责任共担模型下的义务的能力保持透明的云提供商。

免责声明

本报告中的信息“按现状”提供，仅供参考。CISA 和编写机构不认可任何商业产品或服务，包括任何分析主题。通过服务标志、商标、制造商或其他方式对特定商业实体或商业产品、流程或服务的任何提及都不构成也不暗示 CISA 和编写机构对其的认可、推荐或偏袒。本文件是 CISA 的联合倡议，不会自动作为监管文件。

资源

CISA

- CISA的SBOM指南
- CISA的跨部门网络安全性能目标
- 技术互操作性指南
- CISA 和 NIST 对软件供应链攻击的防御
- 不安全技术的代价以及我们可以采取的措施 | CISA
- 停止在网络安全问题上推卸责任：为什么公司必须在技术产品中建立安全性 (foreignaffairs.com)
- CISA的专门针对利益相关者的漏洞分类（SVCC）指南
- CISA 的防网络钓鱼 MFA 资料单
- 小型企业网络指南 | CISA

NSA

- NSA关于内存安全的网络安全信息单
- NSA 的 ESF 保护软件供应链：供应商最佳实践

FBI

- 理解和应对 SolarWinds 供应链攻击：联邦视角
- 网络威胁 – 应对和举报
- FBI的网络战略

美国国家标准与技术研究院 (NIST)

- NIST的数字身份指南
- NIST的网络安全框架
- NIST的安全软件开发框架（SSDF）

澳大利亚网络安全中心 (ACSC)

- ACSC的制造商物联网（IoT)行为准则指南

英国国家网络安全中心 (UK)

- 英国的网络评估框架
- 英国 NCSC 的安全开发和部署指南

- 英国 NCSC 的漏洞管理指南
- 英国 NCSC 的漏洞披露工具包
- 剑桥大学的CHERI
- 《再见，感谢所有的一切》□- NCSC.GOV.UK

加拿大网络安全中心 (CCS)

- CCCS防范软件供应链攻击指南
- 网络供应链：一种评估风险的方法
- 加拿大网络安全中心的 CONTI 勒索软件指南

德国联邦信息安全办公室 (BSI)

- BSI 基准保护纲要 (模块 CON.8)
- 国际标准 IEC 62443，第 4-1 部分
- 2022 年德国 IT 安全状况报告
- BSI 的Web应用程序安全实践

荷兰国家网络安全中心

- NCSC-荷兰成熟身份认证资料单

其它

- 复杂系统如何发生故障
- 复杂系统故障的新面貌