《FIRST-多方漏洞协调和披露指导方针和实践》

V1.1

2020 年春 发布

北京数字观星科技有限公司首译中文版发布。

目　录

一、引言

关于协调漏洞披露的最佳实践、政策和过程的基础性工作主要关注双边协调（例如一名研究者和一名供应商），对多方协调日益增加的复杂性却很少涉及。活跃的开源开发社区、大量的程式错误、增加的供应链复杂性以及 CSIRT 和 PSIRT 所面临的支持挑战等因素只是复杂性的一部分。

通过国家远程通信和信息管理局（NTIA）和 [2]FIRST 的共同努力，形成本文件。本文件的目的是协助改善不同利益相关方社区之间的多方漏洞协调机制。

本文件不同于国际标准化组织漏洞披露和处理标准（国际标准化组织/国际电工技术委员会 29147 和 30111 号标准）。国际标准化组织的标准主要针对一个利害关系人团体，即供应商，以及关注产品漏洞的双边信息披露。本文件是当前最佳实践的集合。该实践将更复杂和典型的现实生活场景考虑进来，即多边漏洞披露机制。

本文件包含一套来自使用实例和示例场景的通用指导思想和最佳实践。本指导思想针对可能同时影响各种各样的供应商以及各种技术漏洞。

注： FIRST.Org 认可本文件。但本文件中的描述仅供参考。因使用本文件而引起的或与相关的损害，FIRST.Org 概不负责。

二、相关方的定义

就本文件而言，以下定义对于在国际标准化组织/国际电工技术委员会 29147：2014 标准中可以找到的定义 [3]，只做略微改动。

◆**公告：**通知、建议和警告产品漏洞的通告或公告。

◆**协调者：**帮助供应商和发现者处理和披露漏洞信息的参与者（可选）。

◆**防御者：**负责防御攻击的利益相关方。一名防御者可以是系统管理员、供应商或防卫技术或服务的提供者。防御者可以检测脆弱的系统、检测并响应攻击，并执行漏洞响应和管理。

◆**披露：**指最初向先前不知情的一方提供漏洞信息的行为。整个披露过程通常涉及多个披露事件。

◆**暴露：**从发现漏洞到漏洞不再被利用之间的时间。

◆**发现者：**识别产品或服务中潜在漏洞的个人或组织。例如，外部安全研究员可作为发现者。

◆**缓解措施：**减少漏洞被利用的可能性或产生负面影响的措施。

◆**修复：**修补、维修、升级、配置或进行文件更改以删除或降低漏洞影响。

◆**供应商：**开发产品或服务，或负责维护产品或服务的个人或组织。

◆**同行供应商：**处于供应链的同一水平的供应商。相同技术（例如 OpenSSL 和 GnuTLS）的独立实现者，或者相同上游技术（例如 Red Hat 和 SuSE）的下游用户都可以是同行供应商。

◆**上游供应商：**向下游供应商提供产品或技术的供应商。

◆**下游供应商：**从上游供应商处获取产品或技术的供应商，将这些产品或技术应用于下游供应商的产品、技术或服务。

◆**漏洞：**可开发利用的软件、硬件或服务的弱点。

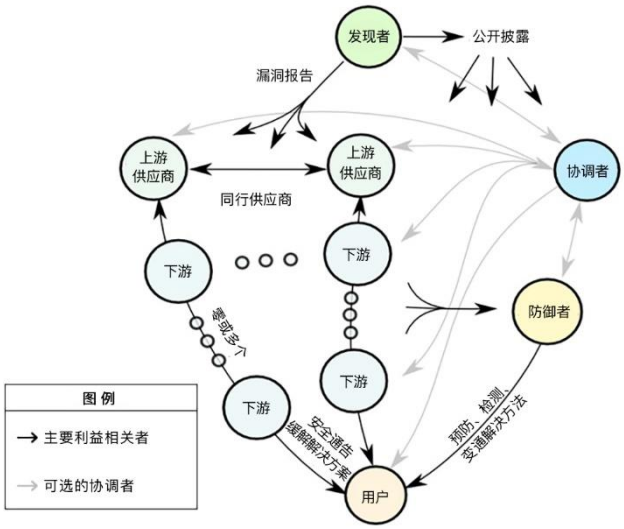

图 1：利益相关者角色和沟通路径

三、指导思想和最优现行方法

下列指导思想源于后面讨论的多方公开使用实例部分中的实例、变量、响应和预防。其中涉及最重要的实践，尤其是那些反复出现的实践。利益相关者应慎重考虑自身的行动，尤其是通知和公开披露漏洞的时候。因为在多方案件中，这些事件会对其他利益相关者造成影响。

（一）建立流程和关系的坚实基础

- 涉及到的各方（尤其是供应商）应制定并公布可采取行动的公共漏洞协调和披露政策和预期，包括披露的时间表和门槛。
- 各方都应该共同发展，随时将同行和其他潜在利益相关者社区的考虑在内。
- 供应商应预先建立上下游供应商的沟通渠道和机制，从而了解潜在的影响和协调时间表。
- 供应商应该追踪第三方控件的使用，以更好地开发库存并理解上游和下游的相关性和依赖关系。

（二）保持清晰的沟通

披露之前

- 对于期望和时间表，各方应该保持清晰沟通，并确保安全性。

- 供应商应该提供当前能够被接受的联系机制，如安全@电子邮件地址和“slash security”(/安全)网页。
- 收到每一次通信，各方应加以确认。
- 就状态更新和对披露时间表的潜在影响，供应商或协调器应和发现者展开频繁沟通。
- 发现者应提供清晰的文档和工具来支持漏洞验证。
- 供应商应清楚地记录产品支持的时间表和限制。
- 各方应避免个体沟通时可能出现的故障点。

披露之后

- 供应商应提供与漏洞修复和缓解有关的报告和公告，而且必须是人眼和机器可读格式（例如通用漏洞报告模板（CVRF）[4]）。
- 除了通过普通的电子邮件(如 secure@example.com)进行沟通外，供应商还应该为上游和下游的利益相关者确定一名专用联系人。
- 如有需要，供应商应该通过协调人员展开多方位的沟通和协调。
- 各方都应利用通用的漏洞跟踪和聚合能力，比如国家标准与技术研究院国家漏洞数据库（NVD）[5]）和通用漏洞列表（CVE[6]）。
- 所有各方，尤其是通用漏洞披露编号机关（CNA），在分配 CVE ID 安全漏洞和填充通用漏洞披露条目时应遵循指南操作。[7]
- 各方均应提供相关信息，帮助其他利益相关方评估与漏洞的严重性、优先级和风险。可参考通用漏洞评分系统（CVSS）。[8]

（三）建立并维持信任

- 各方均应采取措施，确保通讯和处理敏感信息能够保证安全。（例如对利益相关者的通信进行加密）。
- 供应商应在补丁文件发布前严格测试补充资料。
- 供应商可以建立赏金猎人程序、信用或安全港，从而在发布前主动识别漏洞。
- 各方应尽量避免事态升级（包括法律诉讼）。利益相关者应积极倡导安全研究，在相关法律框架内协调披露信息。实际的或可感知的法律或其他强制压力，通常会对安全研究产生寒蝉效应。

（四）尽量减少利益相关者的信息暴露

- 对于经过修复的明确的时间表（例如周二为补丁日），供应商可以发布。
- 可以的话，更新和补丁应该只包括补丁文件，而不包括特定的新功能或非安全错误修正（例如 Java 发布与补丁文件不同的特性变更[9]）。
- 可以的话，供应商应该为用户提供一个自动更新处理过程。
- 如可获得，用户应该启用供应商的自动补丁更新。

- 供应商应该建立并参与信任网路（例如审查邮件列表——比如统一可扩展固件接口同步接收发送器（UEFI USRT）[10]），从而达到快速沟通和协调的目的。
- 供应商可以提供一切可用的缓解措施或变通解决方法，即使这些措施有可能导致服务退化。
- 如使用实例 3，利益相关人应该考虑部分的、初步的公开披露。
- 一旦上游供应商推荐一个新版本，下游供应商应该考虑更新他们的控件。
- 事先没有明确证据公开披露（包括积极开发）的情况下，利益相关者应该为供应商提供合理的禁止披露期以调查和开发修复程序。
- 发布修复程序可能会暴露其他供应商组件中存在的相同漏洞，这一点供应商必须能够意识到。

（五）对早期披露做出快速反应

- 供应商应该分析早期披露的具体情况，并建立优先修复时间表。
- 可能的话，供应商可以联系发现者，确定早期披露的范围并进行损害控制。
- 供应商应针对漏洞和潜在的缓解措施向用户提供沟通，比如可以发布一份临时咨询。

（六）合适的话，发挥好协调者的功用

- 协调者可以帮助联系研究人员、供应商和其他利益相关者。当涉及到多方(供应商)或很难联系到一方(供应商)时，协调者的角色尤其重要。
- 特别是在存在分歧时，协调者可以为研究人员、供应商和其他利益相关者提供额外的技术、影响和范围分析。
- 协调者应发展和保持与其他协调者的关系。
- 应该选择一个协调者作为领导，从而减少涉及多个协调者时的混乱。

四、多方公开使用实例

漏洞披露可能是一个复杂的过程，特别是当涉及到多方(一般是多方供应商)时更为显著。文件的这一部分展示的是一组漏洞披露用例，顺序为从简单到复杂。披露经常偏离预期或理想制程，因此，每个用例中都有变量。在每一种变量中都有原因、预防和回应措施。收集预防和响应作为实践来展示，可用于减少预期变量的发生和成本。

*将实践表示为强烈推荐(“应该”)或建议（“可以”“会”或者“应该可以”）。

*描述多方协调和公开使用实例和变量之后，推荐的实践被收集到总结部分中，形成指导思想和最优现行方法。

（一）用例 0：无漏洞

说明

为了完整起见，这里包含了此类用例。当没有漏洞时，就不需要协调。

（二）用例 1：没有受影响的用户的漏洞

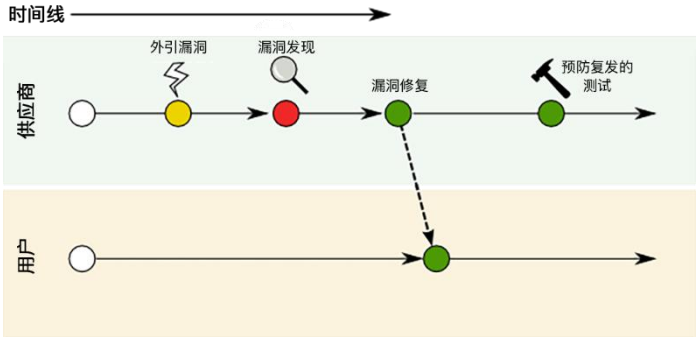

图 2：用例 1，产品有漏洞，但没有受影响的用户

说明

无用户的软件或硬件有存在安全漏洞，但不会以任何方式影响任何人。这种情况的例子包括(a)非生产的、实验性的产品（例如开放式 Web 应用程序安全项目 WebGoat11），(b)内部使用或个人使用，(c)从未发布或出售，或(d)正在开发中。

在产品配置之前发现并修复漏洞。供应商采取措施防止再次出现该漏洞。用户无需咨询。各方无需协调，除非出现以下情况：

- 当漏洞可能存在于类似的产品、协议或算法中时。
- 漏洞代表了一种新的未知的弱点时。
- 无法联系到供应商，但与其他受影响的涉众进行协调。
- 供应商和研究人员不同意。

变体 1：产品在发现或修复漏洞之前配置

说明

产品发布时，有一个或多个现有漏洞。供应商发现漏洞并改正这些漏洞。供应商发布产品的更新版本，并采取措施防止漏洞再次发生。然后由供应商发布一份公告。

原因

- 测试期间未发现漏洞。
- 受影响的产品配置得太快了。
- 使用已知漏洞配置受影响的产品。

预防

- 执行产品渗透测试，并在发布前扫描已知的漏洞。
- 建立赏金猎人程序，在发布前主动识别漏洞。
- 在 beta 质量对比准备的发布需求上设定清晰的期望和基线。

（三）用例 2：存在协调披露的漏洞

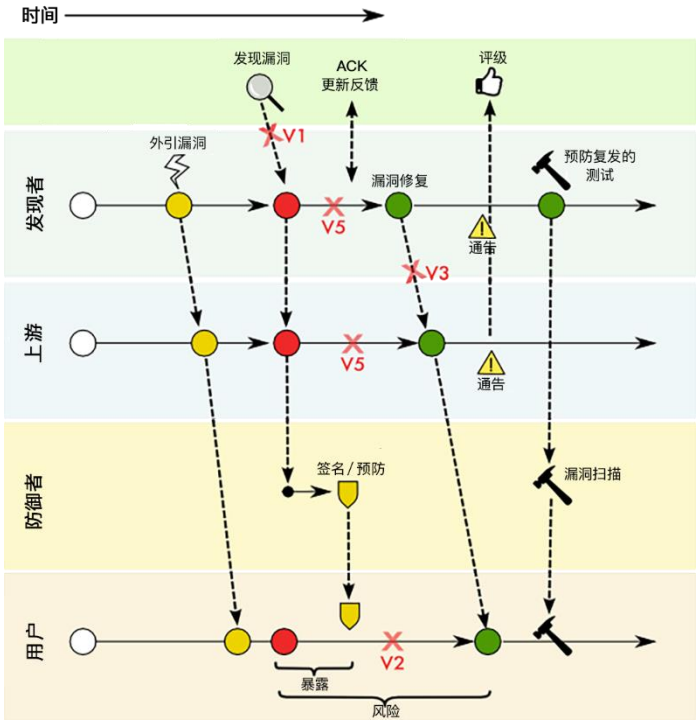

图 3：存在协调披露的漏洞

说明

产品发布后会发现许多安全漏洞。多方利益相关者——包括发现者、上游供应商、供应商、防御者以及用户——参与到协同披露的工作中。鼓励利益相关者遵循 FIRST 和 ISO 等国际机构制定的准则，来制定披露实践的基础。

通用的协调披露过程中，以下利益相关者的角色分别为：

【发现者】：发现者使用标准的漏洞报告通道与供应商联系

【供应商】：解决问题时，供应商会根据需要在适当的时间与上下游供应商沟通。供应商凭正当理由发布公告。

【防御者】：在不包含或推断可能帮助潜在攻击者的信息的情况下，制定缓解措施或备制签名来检测和保护用户不受漏洞的伤害。请求供应商提供相关的测试用例，以检测基于反复出现模式的高级威胁。

【用户】：尽快配置供应商的补丁或缓解措施。

变体 1：进行补救前，发现者公开漏洞细节

说明

有时候发现者可能会在补救之前公开发布漏洞细节，这可能会增加受影响的用户的风险。发现者公开漏洞的原因包括无法与供应商建立联系、财务或其他动机。理想的状态是，在行补救措施之前防止发现者公开漏洞细节，但入如果发现者已经公开了漏洞细节，那么快速响应和提供潜在的缓解措施就至关重要。

原因

- 发现者无法找到供应商联系人。
- 供应商不响应发现者。

- 发现者和供应商对漏洞的界定不一致|（比如，漏洞存在于不受支持的产品版本中，然而却在受支持的产品版本中被修复）。
- 发现者公开为供应商带来发布补丁的压力。
- 发现者为利润所驱动|（比如发现者有出售产品或服务的动力，可以检测或防御漏洞）。
- 公众的认可或名声是发现者的动力。
- 发现者和供应商之间存在不良沟通。
- 发现者对用户安全问题不敏感。
- 发现者认为供应商对用户的安全问题不敏感。
- 对该漏洞的积极利用被发现了。
- 供应商未补救该漏洞。
- 有漏洞的供应商数量太多，供应商无法处理。
- 供应商太过关注与其相关的法律问题。

预防

- 供应商应该提供当前接受的联系机制，如安全@电子邮件地址和“slash security”(/安全)网页。
- 涉及到的各方（包括供应商、发现者和协调器）应相互传达他们的披露计划。
- 所有相关方都应该提供他们的披露政策。
- 经常与发现者应沟通，内容包括定期的状态更新。
- 协调者可以提供对漏洞的分析，并培训供应商或发现者。
- 供应商可以提供安全港、信贷或漏洞奖励等激励措施。
- 各方应尽量避免事态升级（包括法律诉讼）。
- 各方应提倡最低曝光原理。
- 供应商和协调者应该与发现者社区维护一份延伸计划。
- 供应商应避免个体沟通故障点。
- 当涉及大量供应商时，协调者可以支持供应商之间的沟通和协调。

响应

- 联络发现者查看供应商的协调信息披露政策。
- 对发现者表示失望态度，但仍保持积极沟通，同时试图控制进一步的漏洞细节泄漏。
- 供应商可以联系中介。
- 供应商可将内部资源作为最高优先级修补漏洞。
- 如果出现分歧，供应商或查找者可以与协调者进行协调。
- 供应商可以通过最新的安全通告或微博向用户提供缓解建议。

变体 2：用户不会立即配置补救措施

说明

仅提供补救措施不足以降低风险，配置也是十分必要的。比如用户没有配置补救措施，或者在上游供应商提供补救措施后，供应商应立即建议采取缓解措施。总的来说，用户尽可能采用基于风险的方法来决定何时配置供应商提供的补救或缓解措施，以帮助减少潜在的开

发风险。供应商负责关键和高严重性漏洞发布补救或缓解措施时，应尽可能对此类漏洞的可用性进行大范围通报，并提供明确的配置和建议。

原因

- 供应商有提供低质量或不受信任的安全更新的历史。
- 用户担心更改(包括更新)会破坏或减少功能。
- 用户测试和配置需要时间和资源。
- 供应商无法提供自动补丁更新。
- 用户没有启用供应商的自动补丁更新。
- 当安装了较旧的使用周期结束版本或不支持版本，供应商将不会发布该版本的补丁文件程序。
- 用户不完全了解该漏洞的威胁或临界性。
- 用户等待来自供应商的多个打包补丁。
- 用户不知道系统中使用的供应链和控件。

预防

- 对于经过修复的明确的时间表|（例如周二补丁日），供应商可以发布。
- 可以的话，更新补丁应该只包括补丁文件，而不包括特定的新功能或非安全错误修正（例如 Java 发布与补丁文件不同的特性变更 [12]）。
- 可以的话，供应商应该为用户提供一个自动更新处理过程。
- 如果用户能获得供应商提供的补丁，那么应当进行更新。
- 供应商应在补丁发布前严格测试。
- 供应商应该发布他们的安全开发生命周期(SDL)流程的高级版本，并发布公开策略来让用户放心。
- 用户应该从他们的环境中删除使用周期结束的系统和不支持的系统。
- 对无法正确维护和更新的遗留产品版本的延伸支持，供应商应予以消除。
- 确保产品最新的安全通告清楚漏洞的严重性、成功利用的影响以及可用下载的位置。
- 供应商会考虑提供包含第三方控件信息的材料清单。

响应

- 供应商应该采用漏洞评分系统标准化机制——比如通用安全漏洞评分系统，提高用户对漏洞严重性的认识。
- 供应商应该以机器可读的格式提供与漏洞相关的清晰的建议和公告，包括有关修复、补救和缓解的信息。
- 供应商应该提供一切可用的缓解措施或变通解决方法，即使这些措施有可能导致服务退化。
- 可以的话，供应商应该审核用户的环境，并在没有配置补救措施时发送提醒。
- 为关键用户提供一对一支持，打破信任壁垒，并加快采用补救措施。
- 利用现有的客户支持和销售渠道，供应商能够有效地向用户传达安全公告。
- 此外，供应商还可以通过内部通知流程通知客户代表，以鼓励客户申请补救。

变体 3：上下游供应商之间缺乏沟通

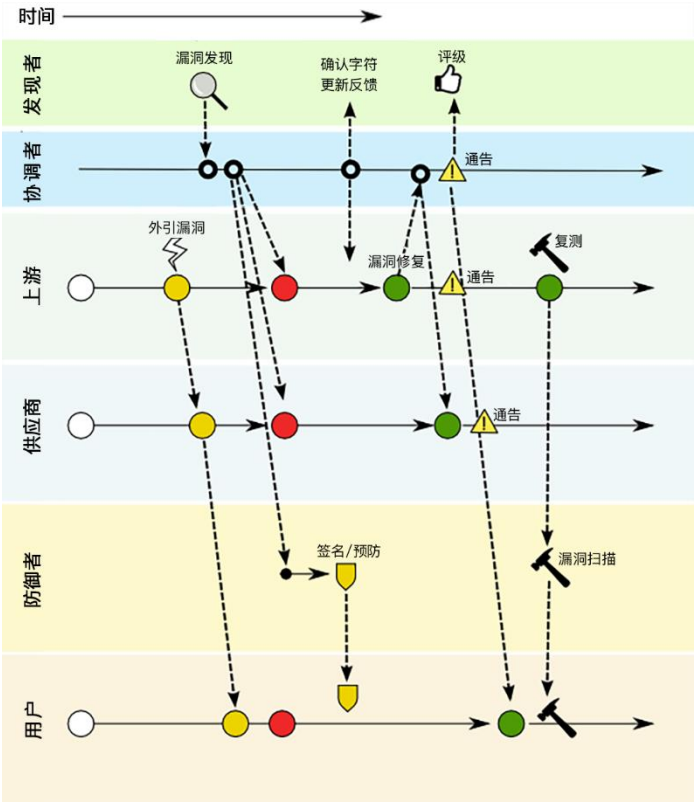

图 4：用例 2 和变体 3-缺乏上下游供应商之间的沟通

说明

上游供应商与下游供应商或供应商与用户之间可能缺少直接沟通或安全披露。在补救的各个阶段，协调者可以很方便地接收和向有关各方分发信息。

原因

- 供应商无法在内部识别漏洞（比如，有可能供应商不会跟踪其产品的第三方控件中的漏洞）。
- 供应商不完全了解或不知晓所有下游涉众。
- 供应商纠正了漏洞，但没有通知所有下游利益相关方。
- 供应商无法预先与下游利益相关者建立可信的通信渠道或保密协议（NDA）。
- 供应商公开披露之前，供应商没有考虑到足够的下游协调和传播时间。
- 供应商没有和已知的下游利益相关者沟通有关漏洞披露的时间表和预期设定等问题。

预防

- 供应商建立可操作的公共漏洞协调和披露政策，理想地描述披露的阈值(如严重性)。
- 供应商应该考虑沟通所有漏洞的补救和缓解信息，而不考虑严重程度或漏洞报告的来源。
- 下游供应商应考虑让其控件与上游推荐的版本保持同步。有选择地为安全漏洞打补丁容易出错，而且源代码可能会在上游和下游实例之间产生差异，那么从长远来看，会产生高昂的代价。下游供应商也可能会错过安全改进或漏洞修复，没有获得通用

漏洞披露赋值或在以后的日期获得漏洞披露赋值（例如通用漏洞披露 2016-2108[13]）。

- 供应商应该追踪第三方控件的使用，以更好地开发库存并理解上游和下游的相关性和依赖关系。
- 供应商应该预先建立一个上下游的信任网路，以便快速沟通和协调（例如邮件列表——比如统一可扩展固件接口同步接收发送器）。
- 供应商应与下游供应商清楚地沟通披露时间表。
- 供应商应该预期已知的下游协调所需的时间框架。
- 供应商可以通过以下方式利用协调者进行沟通和协调，即：
  - 协调者可能从影响多个供应商的发现者收到漏洞报告，然后将该报告分发给受影响的上游和下游供应商。
  - 协调者可以从供应商处接收漏洞报告和相关解决办法，并帮助识别其他受影响的供应商(可能是同行供应商)，并将信息传递给他们。
  - 协调者可以引用供应商目录来确定受影响的供应商。
  - 协调者也可以在适当的时候通知防御者，以帮助减轻漏洞被利用的风险或防止攻击行为。
  - 除供应商的建议之外，协调者还可以发布一份公共建议，以提高对漏洞以及可用补救措施的认识。

响应

- 除了通过普通的电子邮件(如 secure@example.com)进行沟通外，供应商还应该为上游和下游的利益相关者确定一名专用联系人。
- 可以的话，供应商应该向受影响的涉众解释情况，从而增加透明度。
- 供应商应该在漏洞披露之前与受影响的利益相关者协商一个时间框架。
- 供应商应该通过协调人员进行沟通和协调。
- 供应商应该利用常见的漏洞跟踪和聚合功能，如国家漏洞数据库、通用漏洞披露和 FIRST 漏洞数据库目录。[14]

变体 4：进行补救前，供应商公开漏洞细节

说明

多方漏洞披露往往涉及利益相关者之间复杂的相互作用。供应商有可能在补救之前公开漏洞细节。很多情况下，这样的泄露是偶然的，应该制定一个控制损害的计划。事后应对事件进行回顾，以防止今后发生类似事件再次发生。

原因

- 供应商无意间披露。
- 供应商有缺陷或缺乏策略和控制来处理和保护敏感的漏洞相关信息。

预防

- 共享社区可以对违反信任的行为进行惩罚（比如共享社区成员发生漏洞，可能会导致该成员被驱逐出共享社区）。

- 供应商应该演示如何使用已实现的策略和控制来正确管理和限制对敏感漏洞信息的访问（比如符合国际标准化组织/国际电工技术委员会 27001 号标准）。
- 供应商应该实现确保通信通道安全的措施，包括实现对外利益相关者通信进行加密。

响应

- 供应商应该回顾事件以了解原因并减少未来的事件；
- 实施并演示处理敏感信息的新政策；
- 对漏洞信息进行充分的审计和日志记录，以便能够快速和清晰地识别泄漏的根本原因；
- 了解漏洞泄露的原因和地点（防止进一步的破坏时）；
- 此外，供应商应该分析早期披露，并建立优先修复时间表。
- 出于保证透明度和控制损害，供应商应该向公众和受影响的客户发布声明。

变体 5：供应商未修复报告的漏洞

描述

在某些情况下，供应商可能未对漏洞提供补救措施。出现此类情况的原因有很多，包括供应商已不存在、受影响的产品不再受支持、供应商无法验证发现者的报告或供应商未将报告的问题视为漏洞。在报告者和供应商之间建立明确的沟通和对话是制定补救或缓解行动计划的基础。

原因

- 发现者和供应商之间未明确对补救措施和披露的期望。
- 供应商不再存在。
- 供应商选择不修复。供应商不修复和识别漏洞的原因可能有多种，包括：
  - 供应商不再支持该产品。
  - 存在影响修复的兼容性问题。
  - 供应商没有修复此漏洞的资源。
  - 漏洞修复费用过高。
  - 漏洞对供应商的优先级低。
  - 供应商无法验证漏洞。
  - 供应商并不认为报告的问题是漏洞。

预防

- 供应商应清晰记录产品支持的时间线和限制，包括产品生命终止、支持终止和安全支持终止日期。
- 发现者应提供清晰的文档，以便进行漏洞验证。
- 双方（供应商和发现者）应明确沟通和协商期望和时间表，并确认收到每次的沟通内容。

响应

- 供应商可以提供备选的支持产品列表，具有与受影响的已结束生命周期或安全支持的产品相似的功能。

- 供应商应咨询法律人员以解决潜在的责任和赔偿问题。
- 供应商应发布声明，解释未修复漏洞或补救的原因。

变体 6：同行之间缺少沟通协调

描述

同行之间缺少沟通或沟通不畅可能会对协调工作产生负面影响。在某些情况下，因为缺乏对共用组件或技术的用途和影响的认识，导致难以识别和协调受影响的同行。使用第三方协调员，以及培养和维护同行供应商意识，是管理多方协调响应中这些复杂性的两种方法。

示例 1. 名为"httpoxy"的漏洞影响多个 CGI 或类似 CGI 的环境。

据 httpoxy.org，该漏洞最早在 2001 年被发现。多年来，人们多次发现该问题，但从未调查它对其他类似 CGI 的影响。2016 年再次发现该漏洞被利用，人们在各种 CGI 中广泛调查了该问题，并分配了 14 个 CVE ID。

示例 2. CVE-2008-1447

CVE-2008-1447 是 DNS 协议中的一个漏洞，1999 年 djbdns 中的 UDP 源端口随机化理念首次缓解了该漏洞。虽然在公共邮件中强调了这种缓解的重要性，但直到 2008 年，许多其他 DNS 仍未采取这种缓解措施。2008 年演示了针对此漏洞的实际利用，源端口随机化缓解措施才被广泛实施。

原因

- 供应商可能不知道同行供应商使用相同的组件或技术，或者可能不知道所有可能受影响的同类供应商。
- 供应商可能很难识别或协调受影响的同行。
- 供应商可能为保持竞争优势而故意扣留信息。
- 供应商可能无法将问题识别为漏洞（例如，缺少 CVE ID）。

预防

- 供应商应培养和保持同行意识（例如，利用 FIRST 目录来识别同行供应商）。
- 供应商应培养并保持协调意识。
- 供应商应与同行合作，采取安全措施保护普通客户。
- 供应商应识别漏洞并发布出来（例如，分配 CVE ID）。

响应

- 供应商可以聘请协调者。
- 供应商可以选择发布漏洞信息，包括概念验证测试（公开或仅向同类供应商发布）。

变体 7：协调者在补救前公开漏洞详细信息

描述

在此变体中，协调者在修复准备就绪之前公开披露漏洞信息。与以前的变体一样，披露可能是意外的，也可能是因为感知到防御性好处，协调员有意披露。

原因

- 协调者意外披露。
- 由于多个协调者处理相同或类似问题而造成混淆。

- 协调者的禁止披露期（embargo period）到期，或协调者确定供应商未响应。
- 已存在漏洞利用，协调者选择披露。

预防

- 为了减少涉及多个协调员者时的混乱，应选择一个协调者作为牵头人。
- 协调者应具有发展和维护与其他协调者关系的意识。
- 协调者应公布披露政策和期望，包括供应商响应的时间表和期望。
- 协调者和供应商应在流程的早期明确披露时间表。
- 供应者可以选择不与有不协调披露历史的协调者打交道。
- 供应商应协商并依照时间表要求做出响应。

响应

- 供应商可以提高响应流程的优先级。
- 供应商可以发布临时通知。

变体 8：发现者向一家供应商报告一个漏洞，该漏洞可能会影响使用同一组件的其他供应商

描述

在此变体中，发现者发现可能会影响多个供应商产品的漏洞。发现者向一个供应商报告漏洞，但未向其他也受到影响的供应商报告漏洞。其他供应商可能不知道这个问题，而且漏洞解决时客户可能无法获悉。

原因

- 安全研究人员无法知道组件的所有用户，该组件（如开源库）由多个供应商使用。
- 易受攻击的上游组件的供应商可能无法响应，因此发现者向另一个供应商报告，该供应商为此上游组件的用户。

预防

- 接收报告的供应商可以将该漏洞报告给开源库的发布者。
- 如果研究人员向协调员报告，或第一个接到报告的供应商将报告传递给协调者，则此场景可以缓解。
- 如果所有供应商都使用相同的 CVE ID 来描述未修改代码中的同一漏洞，则将有助于客户了解其风险情况。

（四）用例 3：在补救之前公开披露有限的漏洞信息

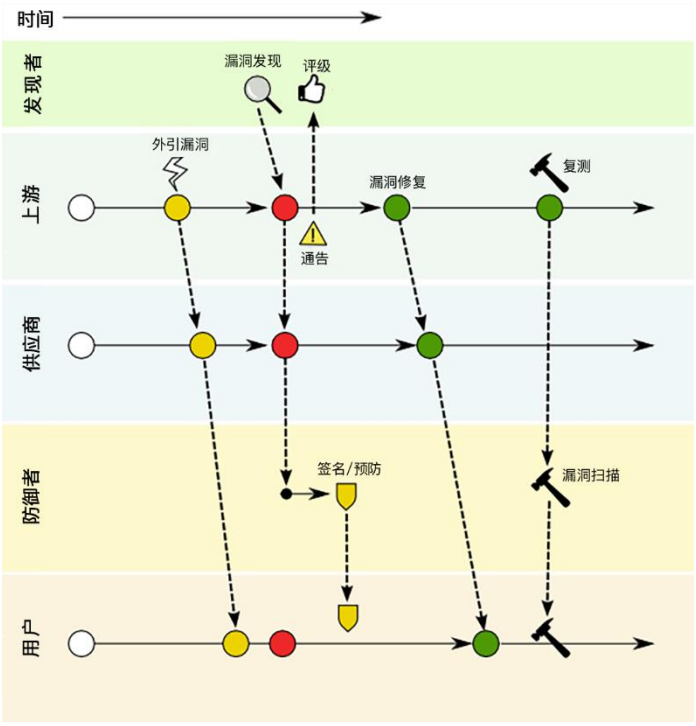

图 5：用例 3 在补救之前公开披露漏洞和影响

描述

发布有关该漏洞的某些信息，而不提供有关漏洞利用的任何提示。此用例不同于通常所称的"完全披露"。

作为完全公开披露和私下协调披露之间的中间途径，发现者或供应商可能会发布一些关于漏洞存在及其披露时间表的初步通知。披露的信息可能包含易受攻击的产品或组件的名称、最坏情况的影响以及未来通报的位置，但不会提供有关利用漏洞的任何提示，例如源代码更改或漏洞类型。当大量供应商受到影响且难以保密时，此披露场景很常见。

此类提前通知可帮助所有响应方（即上游供应商、下游供应商、用户和防范者）对披露响应做规划准备。准备工作可能包括识别可能受影响的产品和资产，确定安全补丁分析人员、代码更改或修补、测试和解决方案交付。用例 2 中的变体（包括原因、预防和响应）也适用于用例 3。

示例 1. 供应商提前警告

2016 年 4 月 28 日，OpenSSL 项目团队宣布了一个新的软件版本，修复了几个"高"严重性安全缺陷，将于 2016 年 5 月 3 日提供。[15]用户和下游供应商有五天时间为采取应对措施做规划和准备，从而最大限度地减少响应者所需的准备时间。

示例 2. 供应商预期节奏

Oracle 根据预先确定的季度计划发布关键补丁更新建议。[16]发布前公告还会在每个关键补丁更新发布前五天发布，并汇总受影响的产品和风险。此通知是客户启动打补丁过程的触发器。

示例 3. 研究员提前警告

[15] https://mta.openssl.org/pipermail/openssl-announce/2016-April/000069.html
[16] http://www.oracle.com/us/support/assurance/leveraging-cpu-wp-164638.pdf

2019 年 7 月 17 日，Orange Tsai 和 Meh Changi 发布了一篇名为《攻击 SSL VPN——第 1 部分：Palo Alto 全球保护上的 PreAuth RCE》的博客文章，使用优步 Uber 作为案例研究！[17] 该帖子提供了一个供应商和产品漏洞的细节，并宣布将在 Black Hat and DEF CON 2019 大会上披露更多内容。

（五）用例 4：在供应商了解漏洞之前公开披露或利用漏洞

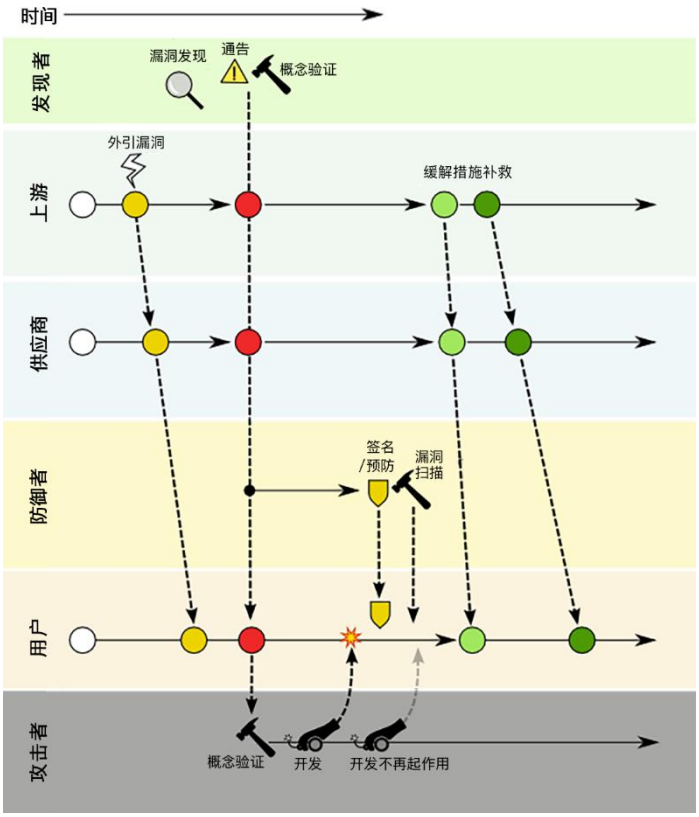

图 6：用例 4 在供应商了解漏洞之前公开披露或利用漏洞

描述

在部署的产品中发现漏洞时，发现者可通过 Internet、邮件列表、学术论文或会议等方法使任何人可以访问有关该漏洞的信息。公开的信息可能包括受影响的产品和版本、可以触发或演示漏洞的概念验证测试用例，以及缺陷或攻击方法的详细说明。此披露并不等待补救或缓解措施的开发部署。此类披露通常称为"完全披露"[18]或"零日披露"。

这种披露方式的主要意图之一是使用户尽早了解该漏洞，以此尽量减少暴露，并假定可能有未知攻击者可能已经知道该漏洞，并可能正在利用该漏洞。

一项对约 400 名研究人员的互联网调查显示，只有 4%的研究人员遵循完全公开披露，而 92%的研究人员遵循某种形式的协调披露。虽然此类披露很少发生，但漏洞响应者（供应商、防御者、用户）应随时准备好处理披露。

[17] http://blog.orange.tw/2019/07/attacking-ssl-vpn-part-1-preauth-rce-on-palo-alto.html
[18] 严格来说，“完全披露”指在提供补救之前公开漏洞信息，不管是在通知供应商之前还是之后。

示例 1. 2015 年 1 月在加利福尼亚州 AppSec 大会上提交的一篇论文[19]描述了与 Apache Commons Collection 相关的在特定场景中的远程代码执行漏洞。Apache Commons 项目事先未得到通知[20]。2015 年 11 月，发表了一篇博客文章[21]，包含基于该论文对多种产品的漏洞利用。在披露之前，没有任何供应商或开源项目接到直接通知。

变体 1：发现者发布漏洞详细信息，之后漏洞被利用

描述

在此变体中，发现者公开披露详细的漏洞信息，而未事先通知供应商。攻击者可以在供应商准备好补救之前使用此信息进行漏洞利用以攻击系统。通常，与供应商开发补救措施和用户部署比较，攻击者开发攻击更快。此变体通常称为"零日"披露。

原因

- 漏洞报告包含概念验证测试或足够的信息，导致该问题的漏洞利用发生。
- 发现者识别以前未知的野外利用并发布。

预防

- 发现者披露时可以隐掉或推迟发布概念证明测试。攻击者必须花费更多时间和精力自主开发漏洞利用，从而为用户自我保护提供时间。
- 发现者可以为有限的受众（包括受影响的供应商）提供概念验证测试。
- 在可能的情况下，在供应商披露通报中添加可追溯性信息可以威慑攻击者。
- 供应商应关注公开披露和讨论。

响应

- 供应商可以提供有关缓解和响应的安全建议。
- 供应商可以加快修补程序测试和发布速度。
- 如果有供应商修复程序可用，用户可以应用。
- 用户可以应用供应商提供的变通方法。
- 用户可以应用内部或外部安全社区推荐的预防或防御变通解决方法。
- 用户可以使用概念验证测试来检查易受攻击的资产。
- 用户可以利用安全最佳实践来限制潜在影响。

变体 2：攻击中使用未披露过的漏洞

描述

在此变体中，由于漏洞在攻击中被使用而变为公开。由于供应商和防御者事先没有发出警告，因此此变体也称为"零日"漏洞或零日利用。这通常是一个非常有害的场景，因为供应商、防御者和用户在受到攻击时匆忙响应。在攻击中的漏洞利用可视为漏洞的披露或漏洞存在的确认。攻击者通常希望漏洞及其利用保持不被发现和不披露状态。

原因

- 不披露或漏洞利用的激励大于为披露而提供的激励。

---

[19] http://frohoff.github.io/appseccali-marshalling-pickles/

[20] https://commons.apache.org/proper/commons-collections/security-reports.html#Apache_Commons_Collections_Security_Vulnerabilities

[21] https://foxglovesecurity.com/2015/11/06/

- 漏洞可能位于恶意软件或僵尸网络中，在这种情况下，泄露可能会使恶意软件更安全。
- 供应商修复不完整，可能会诱使攻击者找到密切相关的漏洞。

预防

- 供应商通常应采取措施提高软件安全性并减少漏洞。此类活动通常称为安全软件开发生命周期（SSDL）或安全开发生命周期（SDL），不在本文档讨论范围内。[22]
- 当通过产品评估发现漏洞或弱点时，应向适当的利益相关者报告所有发现的问题并加以解决。攻击者可能使用相同的安全评估工具和技术，并且可能遇到同样的问题。
- 为了防止恶意修改，维护供应链完整性，供应商应生产防篡改或篡改留痕产品。
- 源代码或软件的真实性应使用强加密（例如，在分发软件时使用数字签名或HTTPS）进行验证。下游供应商应验证其产品中包含的组件的真实性。
- 在可能的情况下，产品应默认启用签名、信任和验证执行。
- 用户应验证要使用或部署的产品的真实性。
- 用户和防御者应持续检查其部署有无未授权更改或异常。
- 仔细检查退回或停用的产品是否有安全妥协迹象。

Response 响应

- 供应商和防御者应分析利用利用情况以确定漏洞。
- 在适当情况下，供应商应考虑提供包含以下安全通告：
  - 承认问题;
  - 补救的开发状态;
  - 可能的缓解措施和变通解决方法。
- 供应商可以加快修补程序测试和发布速度。
- 用户应用供应商修复程序（如果可用）。
- 用户应用供应商提供的变通解决方法。
- 用户可应用内部或外部安全社区建议的预防或防御变通解决方法。
- 用户可以利用安全最佳实践来限制潜在影响。
- 在确定任何评估（内部评估或客户评估）发现的漏洞或弱点的优先级时，供应商应考虑攻击者可以找到相同或类似的漏洞。
- 如果防御者发现事件指标，则应将这些指标报告给适当的供应商或利益相关者进行调查。

致谢

漏洞协调特殊兴趣小组（SIG） 感谢所有成员，特别是以下贡献者：

Pete Allor

Christa Anderson, Microsoft

Jerry Bryant, Intel

Vic Chung, SAP

[22] 协调的漏洞披露常被认为是安全软件开发生命周期（SSDL）的部署，维护，支持阶段的一部分。

Mark Cox, Red Hat

Jeroen van der Ham, NCSC-NL

Jean-Robert Hountomey, Brocade

Kent Landfield, McAfee

Magid Latif, Intel

Art Manion, CERT/CC

Klee Michaelis, Cisco

Beverly Miller Alvarez, Lenovo

Bruce Monroe, Intel

Chandan Nandakumaraiah, Palo Alto Networks

Kymberlee Price, Bugcrowd

Shawn Richardson, NVIDIA

Vivian Smith, Dell Technologies

Katie Trimble Noble, Intel

Krassimir Tzvetanov

Tania Ward, Dell Technologies

Brian Willis, Intel

SIG 还要感谢美国商务部国家电信和信息管理局（NTIA）的 Allan Friedman。