简译版

修复一个漏洞平均耗时 38 天

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	It Takes an Average 38 Days to Patch a Vulnerability		
原文作者	Kelly Sheridan	**原文发布日期**	2018 年 8 月 22 日
作者简介	Kelly Sheridan 是 Dark Reading 的编辑。https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/it-takes-an-average-38-days-to-patch-a-vulnerability/d/d-id/1332638		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

修复一个漏洞平均耗时 38 天

Kelly Sheridan

2018 年 8 月 22 日

通过分析超过 3.16 亿起安全事件，tCell 公司发现了 AWS 和 Azure 云生态系统中 Web 应用程序最常遭遇的攻击类型。

根据一项关于 Web 应用程序攻击趋势的新报告，普通组织需要一个多月才能修复最严重的漏洞。

这些数据来自 tCell 公司发布的 2018 年第 2 季度《Web 应用程序安全报告》。该公司研究人员分析了超过 3.16 亿起客户安全事件，并公布了在亚马逊 Web 服务（AWS）和微软 Azure 云生态系统中，Web 应用程序最常遭遇的攻击类型。

该公司联合创始人兼首席执行官迈克尔·费尔塔格（Michael Feiertag）解释说，去年 tCell 发现“成功攻击”/“攻击尝试”的比例较高，因此首次发布了此报告。他说，通常，在攻击者的 10 万次攻击尝试中，只有 1 次能够成功。鉴于攻击者使用自动化手段来捕获 Web 应用程序中的漏洞，因此此类攻击噪声较多。

“我们评估了上一季度的数据，以了解通过这些应用程序访问安全数据，会如何影响安全团队对它们的保护。”他继续说道，“我们发现，获得这些数据的安全团队显著改善了漏洞修复流程，他们使用这些数据来改善与开发人员和运营同行的协作，确定工作的优先级，从而扩展他们的能力。”

研究人员发现了两种主要的攻击方式。第一种是针对应用程序用户的跨站点脚本（XSS）攻击，这是最常见的攻击类型。他们指出，大多数 XSS 实例只是攻击尝试。去年，在 1200 次 XSS 攻击尝试中只有 1 次能够获得成功，因此我们很难将成功攻击和攻击企图区分开来。

第二种是 SQL 注入攻击，攻击者通过这种方法访问敏感数据或运行 OS 命令，以进一步访问目标系统。在第 2 季度 TOP 5 Web 应用攻击中，其他三种攻击分别是自动化威胁、路径遍历和命令注入。

“我们发现，攻击出现了两极分化：大规模扫描攻击和针对性攻击。”费尔塔格说。大多数是扫描攻击，这些攻击针对多款应用程序，不放过任何可能的攻击机会。研究人员还发

现，针对性攻击的数量激增，这些攻击利用高级威胁手段，试图寻找一些应用程序中的高价值漏洞：例如，通过命令注入将恶意代码注入服务器，或者利用受感染的凭证获取管理员访问权限。

“两者似乎都出于经济动机，但采用不同的方法来实现目标——前者关注攻击的广度，后者则更关注攻击的深度。”他补充道。

TCell 列出的 TOP 5 攻击类型不同于开放 Web 软件安全计划（OWASP）列出的类型。后者列出的 TOP 5 攻击类型是：注入攻击、破解身份验证、敏感数据泄露、XML 外部实体攻击和破解访问控制。费尔塔格解释说，两者不同的原因是，tCell 只考虑公共云环境中 Web 应用的攻击，而 OWASP 则考虑了更广泛的数据集，他们“从不同的视角看待同一个问题”。

CVE 漏洞：普遍存在和打补丁

根据 tCell 的报告，在第 2 季度，90％的活跃应用程序都存在已知的 CVE 漏洞，30％则存在严重的 CVE 漏洞。专家们在报告中解释说，每个应用程序平均检测到 2900 个路径或暴露的 API 端点，这就是它们的攻击面，代表着安全“盲点”。

组织修复 1 个漏洞平均需要 38 天（无论其严重程度如何），而修复最严重的 CVE 漏洞则需要 34 天。研究人员指出，这些统计数据可能会受到组织规模的影响——相比于小企业，大企业需要更长的时间来修复漏洞。

漏洞的严重程度越低，修复所需的时间则越长。修复“中等”严重程度的漏洞平均需要 39 天，修复“低”严重程度的漏洞需要 54 天；而修复最老的、未打补丁的 CVE 漏洞则需要将近 1 年的时间（340 天）。

费尔塔格说，修复漏洞所需的时间正在变短。他指出，随着安全团队意识到快速打补丁的重要性，“客户大大减少了修复漏洞的耗时”。

Web 应用安全：公司在做什么

费尔塔格表示，前瞻性的公司正在采用与 DevOps 和云集成的应用安全方法。实现这一目标的技术（如 RASP [实时应用程序自我保护]）更加新颖，仍在不断发展，是对 WAF（Web 应用安全防火墙）、AST（应用安全测试）和 Waterfall SDLC（软件生命周期瀑布模型）流程的改进。

然而，他继续说道，许多团队和公司还未接受这种变化，已经落后。他们的安全工具和策略赶不上其软件和基础设施的发展。

“讽刺的是，这些通常是在安全方面投资最多的公司，但他们所取得的安全成果通常低于更灵活、更高效的同行。”费尔塔格说。他建议公司了解具体的风险。“如果你有一个 Web 应用程序，那么它最终会受到攻击。”他说，公司可以使用正确的工具和数据将攻击风险降至最低。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*