每周安全事件

内 容	
中文标题	Systemd 套件漏洞可以导致运行 Linux 的计算机崩溃
英文标题	Systemd flaw could cause the crash or hijack of vulnerable Linux machines
作者及单位	Pierluigi Paganini
内容概述	谷歌安全团队的 Felix Wilhelm 披露开源 Systemd 管理套件的 DHCPv6 客户端中存在漏洞，攻击者可以使用恶意制作的 DHCPv6 数据包触发漏洞并修改易受攻击系统的部分内存，从而可能导致远程执行代码。该漏洞被追踪为 CVE-2018-15688。Wilhelm 称函数 dhcp6_option_append_ia 用于将服务器接收到的身份关联编码到传出 DHCPv6 包的选项缓冲区中，攻击者可以使用服务器 id 大于等于 493 字符的 DHCPv6 服务器触发溢出。Systemd 套件存在多个 Linux 发行版，专家指出通过网络或 ISP 中恶意 DHCPv6 服务器发送特制路由器通告消息，启用 DHCPv6 客户端可劫持或基于 Systemd 的 Linux 计算机崩溃。Systemd 开发者及时发布了安全修复程序。
链接地址	https://securityaffairs.co/wordpress/77470/hacking/systemd-security-flaw.html

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.SpamSms.a[exp,rog] 2018-10-26	该应用程序伪装正常应用，运行联网获取参数私自发送指定短信，监听、拦截短信，造成用户资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SpyApp.s[prv,mat,spy] 2018-10-27	该应用程序伪装成系统应用，运行后激活设备管理器，接收远程指令，可获取手机位置、短信记录、通话记录、联系人信息及 Gtalk、Skype、Facebook、Yahoo、WhatsApp 等社交应用消息记录上传远程服务器，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Spyoo.g[prv,spy] 2018-10-28	该应用程序是一款间谍软件，运行后私自提权，窃取用户短信、联系人、通话记录、地理位置、浏览器历史记录、社交软件信息、私自录音、录像，并将用户隐私上传至服务器，造成用户隐私泄露，建议立即卸载。（威胁等级中）
	较为活跃样本	G-Ware/Android.jiasuo.da[rog,sys,lck]	该应用程序伪装正常应用，请求用户激活设备管理器，篡改界面欺骗用户付费解锁，造成用户设备无法正常使用，建议不要使用。（威胁等级中）
		RiskWare/Android.E4Acili.a[exp]	该应用程序是一个[illegible]，诱导用户加入 QQ 群，部分功能需要购买后才可使用，存在一定的风险，[illegible]使用。（威胁等级低）
		Trojan/Android.Locker.bd[rog,sys,lck]	该应用程序伪装游戏外挂辅助类工具，诱导用户获取 root 权限，而后篡改锁屏界面，破坏用户付费解锁，影响用户手机的正常使用，建议不要使用。（威胁等级中）
		G-Ware/Android.Dropper.br[exp,rog]	该应用程序经过重打包处理，运行后会激活设备管理器，释放恶意子包，释放子包私自下载其他应用，加载广告，造成用户流量消耗，建议不要使用。（威胁等级低）
		Trojan/Android.adups.b[exp,bkd,tmt]	该应用程序[illegible]，[illegible]存在执行指定命令的功能，私自提权[illegible]，静默安装，私自启动本地文件，造成用户手机流量消耗，存在安全隐患，建议删除。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 权限提升漏洞（CVE-2018-15967）	[illegible]Adobe Flash Player，[illegible]（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Wimmer	此威胁是一种有广告行为的灰色软件类程序，该家族通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户可能并推送广告。（威胁等级低）
		RiskWare[Downloader]/Win32.Kasimr	此威胁是一种下载广告软件的风险软件类程序。该家族会自动下载并运行用户不知情或不允许安装的软件，同时它也可以不断地检查更新文件本身。（威胁等级低）
		Trojan[Exploit]/JS.Agent	此威胁是一种使用 JS 脚本语言编写的，可以利用漏洞下载恶意代码的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，持大量基因片段定性的恶意代码样本。（威胁等级中）
		GrayWare[AdWare]/Win32.IBryte	此威胁是一种广告类程序，该家族样本运行后连接远程服务器下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级低）
		Trojan[Rootkit]/Boot.Cidox	此威胁是一种可以感染 MBR 并在系统与核之前加载的木马家族。该家族通常以正常的应用程序伪装，会[illegible]，[illegible]，在电脑中留下隐藏的后门，并试图攻击局域网内的其他机器。（威胁等级高）

如何控制供应商风险：六步走

Jeff Rowley, Sara Laverick/ 文　安天技术公益翻译组 / 译

要想掌控公司面临的风险，你需要了解第三方供应商所带来的风险。

这听起来可能很简单，但是，除非你能够持续追踪第三方供应商，否则你就无法了解他们带来的网络安全和技术风险。

追踪供应商风险是一项艰巨的任务，需要付出大量的时间和资金，可能会超出公司的承受能力。但是，考虑到众多的网络安全威胁，以及各类[illegible]网络风险和数据泄露的法规，密切关注供应商风险[illegible]方必要。

许多公司与第三方供应商合作，以实现关键业务功能并提高运营效率。然而，这些供应商可能是网络安全和技术风险的重要源头。

最近的报告表明，第三方数据泄露是最常见、代价最高的网络事件类型。对大型企业而言，发生事件后的平均恢复成本接近 123 万美元，而且这一数字正在以每年高达 35% 的比例增长。能够访问企业敏感数据的供应商（如金融服务公司、“软件即服务”[SaaS] 提供商和数据存储公司）可能会给企业带来严重的风险。

但是，在追踪和处理第三方供应商风险方面，许多公司仍然挣扎在分配必要的时间或资源上。因此，这些公司无法完全了解他们有多少供应商，或者他们暴露的数据量。Ponemon Institute 最近的一份报告显示，只有 33% 的公司会跟踪第三方供应商清单，并持续评估供应商可以访问的公司数据。

如何追踪供应商风险

控制供应商风险的关键是：保持完整的供应商风险跟踪清单；其挑战在于：如何利用[illegible]

以通过以下六个措施来掌握供应商的情况，充[illegible]

1. 考虑到每个供应商

你可能拥有完整供应商的清单，或者部分供应商的清单。重要的是，要及时更新供应商清单，保持其完整性和全面性。与公司的会计部门以及负责采购的人员核实供应商信息——在清单中删除重复项或不再合作的供应商。要[illegible]中，应该限制其直接在公司的系统中更新其信息的权限（这些信息包括但不限于其 logo、地址、产品、服务以及分支机构等）。

2. 集中管理供应商清单

公司应该集中管理供应商清单，并确保这些清单能够轻松访问。各公司可以指定专人来维护清单，由高层管理人员对其授权并在整个公司公示。此外，公司还可以根据需要使用专用的供应商管理技术解决方案。

3. 对供应商进行尽职调查

公司应对每个供应商的网络安全实践进行评估，确定这些安全实践是否与自己的一致。优先评估能够访问公司敏感数据或可能导致运营风险的供应商，包括其保护措施、事件响应计划、业务连续性计划等等。

4. 评估供应商风险

[illegible]让相关业务部门对供应商的重要性进行排名（例如，关键、重要、有用或多余）。让公司的网络安全团队（或者至少是 IT 团队）分析[illegible]

5. 定期、持续地追踪和处理供应商风险

通过控制供应商风险来保护公司需要持续不断的努力。不可以“三天打鱼两天晒网”——例如，今天记录了供应商风险，以后就不再维护和更新了。控制供应商风险的关键是持续追踪和严密监测。为了降低风险，请将[illegible]供应商风险[illegible]作为一项常规工作。如果他们[illegible]为公司提供关键服务，[illegible]

就像你与供应商签订合同来处理专业任务一样，请考虑采用相同的策略来管理供应商风险——可以将供应商管理外包给专门监控供应商、跟进其尽职调查的公司。这些公司拥有丰富的经验和专业知识，能够高效和有效地执行此类工作，从而节省你的时间、资金和精力。获取专业公司的帮助，是大幅降低网络安全和技术风险的好办法。

追踪供应商风险，保护公司安全

各公司都致力于降低其网络安全和技术风险，上述措施能够帮助他们牵制网络犯罪分子和其他不良行为者，避免由于违规而受到监管机构的处罚。

要想控制供应商风险，你首先需要了解第三方供应商[illegible]带来的风险。为此，请保持公司供应商的完整清单，不断更新和完善清单，并持续进行[illegible]。此外，还需要对供应商风险进行排名，并跟进其尽职调查。各公司应将追踪供应商风险作为一项常规性和持续性工作，或者将此类工作外包给专业公司。通过这些措施，公司可以控制供应商风险，保护自己的利益。

作者简介　Jeff Rowley, Sara Lavenck。Jeff Rowley 和 Sara Laverick 是 ACA Aponix 公司的首席顾问。

原文信息　2018 年 10 月 24 日发布于 Information Week
原文地址 https://www.informationweek.com/strategic-cio/security-and-risk-strategy/taking-control-of-vendor-risk-a-6-step-approach/d/d-id/1333108

免责声明　本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。[illegible]同时对所获得原文[illegible]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[illegible]

本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的[illegible]承担。