OUCH!2020年5月

SANS SECURITY AWARENESS

OUCH!

给大家的安全意识通讯月刊

更新的作用

概述

你可能有所不知，网络攻击者时时刻刻都在人们日常使用的软件中寻找和发掘新的漏洞和弱点。这些软件可能是笔记本电脑上运行的软件，可能是智能手机上的移动应用程序，甚至可能是婴儿监护仪或其他家庭设备中的软件。不法分子利用这些软件弱点，远程侵入世界各地的设备。与此同时，软件和设备供应商也在不断开发针对这些漏洞的修补程序，并以软件更新的形式发布修补程序。自我保护的最佳方式之一就是确保使用的所有技术都安装了最新的更新，从而大大增加网络攻击者的破解难度。

更新的工作原理

当供应商发现软件漏洞后，他们会开发并发布软件更新（也称为补丁）。如今的大多数软件程序和设备都有一种机制，可以通过互联网连接到供应商的服务器以获取软件更新。这种更新其实就是一个小程序，通常会自行安装并修复漏洞。举例而言，用来运行笔记本电脑（例如Microsoft Windows或MacOS）或运行智能手机（例如Android或iOS）的操作系统就是你需要更新的软件。此外，你还需要更新设备上运行的程序，例如笔记本电脑的Web浏览器、文字处理器、消息传递软件或手机上的移动应用程序（尤其是社交媒体应用程序）——人们往往会忽略这一点。

因此，每当你购买新的计算机程序或新的移动应用程序时，请先查实软件供应商是否会经常更新程序或设备。软件不更新的时间越长，就越有可能产生让网络罪犯有机可趁的漏洞。正因如此，包括Microsoft在内的许多供应商至少每个月都会自动发布新补丁。

最后一点，如果你不再使用某些计算机程序、软件或移动应用程序，请记得从系统中删除。需要更新的软件越少，你就越安全。

更新

一般而言，更新系统有两种方法：

- **自动更新：**当设备、操作系统、程序或移动应用程序检测到供应商发布新的更新时，它会自动下载并安装更新。自动更新的好处是不需要执行任何操作。软件会确保你使用的技术是最新的。自动更新的缺点是更新后的程序可能会引发某些问题，从而导致功能丧失或数据丢失。对于个人设备而言，这种情况很少见，但在大型公司等更复杂的环境中，这种情况却时有发生。

- **手动更新：** 当设备、操作系统、程序或移动应用程序有更新可用时，你必须手动下载并安装更新。这种方式让你可以更好地控制要安装什么更新、何时安装。医院或公用事业单位等大型组织通常倾向于手动更新，因为手动更新让他们可以先对更改进行测试，以检测并解决由更新引起的任何问题。手动更新的缺点是更新系统可能耗时较长，你甚至可能会忘记安装更新。

结论

对个人、家庭和小企业而言，强烈建议你在所有设备上启用自动更新。这样可以确保你使用的所有技术——从智能手机和笔记本电脑到婴儿监护仪和门锁——都安装了最新软件。经过更新的设备和软件会大大增加不法分子的攻击难度。要想保护自己并安全使用当今的大多数技术，最简单、最有效的方法之一就是启用自动更新。

特邀编辑

Don C Weber是信息安全领域的权威人士，自2002年以来在DFIR、渗透测试、研究和管理方面积累了丰富的经验。Don加入了SANS咨询委员会、道德委员会、金牌计划，目前是ICS410的讲师。Don的联系方式如下：@cutaway和https://www.cutawaysecurity.com.

资源

备份重要信息：https://www.sans.org/security-awareness-training/resources/got-backups
保持安全的四个简单步骤：
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

由以下人士为本社区贡献翻译：Donny Wang