2016 年 8 月 4 日，星期四

漏洞聚焦：Hancom Hangul Office 中发现多个任意代码执行漏洞

漏洞发现者：Talos 漏洞研究团队。作者：Alex Chiu。

保护网络和环境的安全是一项富有挑战性的任务，如果组织需要跟踪每天使用的各种软件包，则更是如此。在各类软件（如操作系统、浏览器和防病毒软件）中，像 Hancom Hangul Office 这样的生产力套件可以说是组织需要跟踪和修补的重要软件的典型代表之一。Talos 致力于帮助我们的客户通过各种方式（例如识别重要软件包中的零日漏洞）尽可能确保安全性。日前，Hancom 披露了由 Talos 发现和报告的 8 个任意代码执行漏洞。Hancom 已发布了解决这些漏洞的软件更新，Talos 对 Hancom 给予的合作表示诚挚的感谢。

Hancom Office 是一款世界通用的软件，在韩国尽人皆知，广泛用于各种政府组织、公共机构和非政府组织。实际上，韩国政府之前已指定 Hancom Office 作为政府系统使用的官方生产力套件。据估计，Hancom 在韩国的生产力套件市场份额约为 30%。

Hancom Office 拥有庞大的客户群，当然也吸引了攻击者利用其发起攻击。据称，朝鲜政府是利用 Hangul Word Processor 漏洞发起若干针对性攻击的幕后黑手。有其他公司曾于 2013 年和 2015 年记录过此类事件。此外，Hancom 始终积极寻求扩大在韩国和海外的市场份额。

漏洞详细信息

Hancom Office 的 Hcell 和 Hshow 中存在多个漏洞，通过利用这些漏洞，攻击者可以在受感染的用户设备上执行任意代码。如果用户打开经过精心伪装并可利用这些漏洞的 Hshow (.hpt) 文件或 Hcell (.cell) 文件，攻击者便可以利用这些漏洞，在当前用户环境中执行选择的任意代码。利用漏洞的可能场景包括垃圾邮件和网络钓鱼活动，或者托管用户生成内容的网站（攻击者可能会诱导用户在用户主机上下载并打开相关内容）。

Talos 在 Hancom Office 套件中发现的各个漏洞列出如下。有关各个漏洞的更多详情，请参阅相关的漏洞报告或访问我们网站上的漏洞报告门户。

Hancom Office HShow

- TALOS-2016-0144 - Hangul HShow 未指定的架构性整数堆缓冲区溢出漏洞
- TALOS-2016-0145 - Hangul HShow 未指定的架构性整数堆缓冲区溢出漏洞
- TALOS-2016-0146 - Hangul HShow 未指定的架构性整数堆缓冲区溢出漏洞
- TALOS-2016-0147 - Hangul HShow 未指定的架构性基于堆的越界写入漏洞

Hancom Office Hcell

- TALOS-2016-0148 - Hangul HCell Workbook Table 和 Pivot Styles (0x088e) 基于堆的缓冲区溢出漏洞
- TALOS-2016-0149 - Hangul HCell OfficeArt Record (0x00ec) pConnectionSites 和 pVertices 基于堆的缓冲区溢出漏洞
- TALOS-2016-0150 - Hangul HCell HncChart 0x7ef0 CFormulaTokenSizeModifier 索引溢出漏洞
- TALOS-2016-0151 - Hangul HCell CSSValFormat::CheckUnderbar Off-by-one 基于堆的缓冲区溢出漏洞

已知存在漏洞的版本

目前，Talos 只确认了这些漏洞存在于以下 Hancom Office 版本：
Hancom Office 2014 VP

总结

要缓解危害风险，组织势必需要适度加大防御投入并增强风险意识。为此，组织需要注意两点，一是努力全面地识别、记录和修补所有在用的通用软件包，二是确保遵循安全开发实践。同样重要的是，防御者需要帮助识别软件包中的漏洞并认真负责地进行披露。

Talos 将本着负责任的态度进行零日漏洞识别，一如既往地开展此领域的研究、调查工作，并认真负责地进行披露。通过开发编程方法识别零日漏洞，同时确保解决这些漏洞，这对于提高互联网安全性非常重要。如此一来，我们就可以获得有价值的见解，了解如何改进自己的开发实践以及如何帮助确保可能会遭到攻击者利用的软件的安全。

覆盖

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
WSA	✔

以下 Snort 规则可检测 HPT 和 CELL 文件的攻击尝试：
38856-38859、38868-38869、39049-39050、39110-39111、39757-39762

如需获取零日漏洞或漏洞报告的详细信息以及相关信息，请访问：
http://www.talosintelligence.com/vulnerability-reports/

发布者：Alexander Chiu；发布时间：下午 2:09
标签：公告、Hancom、Hangul、Office、修补、漏洞研究