新型 0-day 漏洞影响 IE 浏览器　趋势科技虚拟补丁助用户脱离险境

停止服务后的 Windows XP 将受直接影响　让消费者和企业更容易受到威胁

[趋势科技中国]– [2014 年 4 月 30 日]近日，微软发布了一个安全公告：2963983，其指出当前所有主流版本的 Internet Explorer 浏览器（IE6~IE11）均存在 0-day（零日攻击）漏洞，这成为第一个会影响 Windows XP 系统而不会被修补的漏洞，将可能导致内存崩溃，使攻击者能够在当前用户账户下执行恶意代码！截止目前，趋势科技已在漏洞公告两天内 (4/29-4/30)将虚拟补丁自动推送给所有部署了趋势科技 Deep Security（服务器防护）、OfficeScan IDF（终端防护）或 Deep Edge（网关防护）等解决方案的用户。此外，趋势科技威胁发现设备 TDA 也在已更新的病毒码中会包含了对于此漏洞攻击行为的检测，在攻击还没有造成破坏之前，帮助用户全面、及时的找出安全威胁。

趋势科技此前已经发出过预警，使用 Windows XP 的风险将会与日俱增，此次漏洞事件已证明了这一点。这意味着数以千万仍在使用该操作系统的消费者将会面临一个永远不会被完全修复的安全漏洞。

据微软安全公告指出，此次漏洞属于远程执行恶意代码的 0-day 漏洞，当 IE 浏览器访问已删除的或是未正常分配的内存对象时可触发漏洞。该漏洞可能导致内存崩溃，从而使攻击者能够在当前用户下执行恶意代码，攻击者可以构造一个具有特殊代码的 Web 页面诱使用户访问并进行漏洞攻击。由于该漏洞威胁所有主流版本的 IE 浏览器，且目前并无官方的解决方案，所以用户的网络安全将受到极大的威胁。

趋势科技企业业务部产品开发总裁刘硕琛指出：“0-Day 对网络安全的真正威胁是最可怕的，因为这种风险不易察觉。而从理论上讲，由于系统中的漏洞几乎不可避免，而且其发现在多数情况下都会领先于解决方案的提出，所以弥补措施几乎永远滞后。尽管微软已经停止了对 Windows XP 的支持，但仍然存在一些解决方案来解决或减轻这一威胁。要防范 0-Day 漏洞的威胁，用户需要采取适当的方式来降低安全事故发生的几率，并使用趋势科技虚拟补丁等解决方案来争取时间。“

此外，趋势科技提醒用户可以遵循以下几点建议来降低该漏洞对网络安全的威胁：

1、 部署微软增强的缓解体验工具包 4.1：http://support.microsoft.com/kb/2458544/zh-cn

2、 启用 IE 浏览器中的增强防护模式，将 IE 浏览器安全设置级别选择为“高”，以阻止 Script 和 Activex 在后台运行。(注意 :改设置可能影响正常插件的安装和使用 ,请将确认安全的站点加入受信任站点中)

3、 在微软 Outlook 、Outlook Express 中打开 HTML 邮件受限站点区域，会禁用脚本以及 Activex 插件，该功能也可以降低漏洞执行恶意代码的风险。

4、 不要随意访问不明链接：该漏洞无法使用户主动访问恶意站点，所以攻击者在利用此漏洞时必须引诱用户访问他们构造的恶意站点，所以加强用户的防范意识不要随意访问或点击不明链接也能够降低风险。

5、 取消注册 VGX.dll，对 VGX.dll 设置更加严格的访问控制策略。由于取消注册 VGX.dll 后将会导致 VMX 无法显示，可以通过命令恢复注册 VGX.dll。

6、 通过趋势科技 Deep Security 、OfficeScan IDF、Deep Edge 等解决方案，使用虚拟补丁防护功能来降低威胁。趋势科技虚拟补丁已在漏洞发布两天内自动推送给用户，适用多产品、多形式的部属，并且适用于各种客户环境且不影响客户端的操作系统，保护范围包括 Windows XP 系统。更为重要的是，虚拟补丁为用户赢得数星期或数个月的处理时间，防止系统遭到攻击，让 IT 人员按照既定的时程来完整测试并部署软件修补程序，这将有效提升系统的安全性。

7、 对于黑客可能利用漏洞进行的攻击，趋势科技威胁发现设备 TDA 可以帮助企业用户获取领先一步的洞察力与防御力，并强化现有的信息安全防护措施并与其整合，形成一套完整且针对客户环境量身定制的个性化防御方案。通过 TDA 内建的高级威胁扫瞄引擎（ATSE）能够检测含有此漏洞攻击代码的恶意行为，能够在攻击还没有造成破坏之前，利用增强的威胁引擎和多级关联规则具有一流的检测功能，全面、及时的监测出安全威胁。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn 。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。