**网络安全监测工作动态**

2018第1期（总第1期）

 陕西省网络与信息安全测评中心 3月1日-3月31日

本月，陕西省网络与信息安全测评中心（以下简称“测评中心”）对受委托的257个政府网站进行了安全监测，共发现无法正常访问的政府网站3个，被恶意篡改的政府网站11个，存在严重高危漏洞的政府网站50个。从安全防御情况来看，目前针对我省政府网站的境外攻击主要来自于保加利亚、俄罗斯、美国、韩国等国家和地区，占攻击总数的4.07%，攻击手法主要为恶意扫描、CC攻击、XSS攻击等。

一、安全监测情况分析

（一）可用性监测情况

共监测发现3个网站存在无法访问情况，主要集中在各市级政府网站，主要原因为网站服务器异常，导致网站服务暂时中断。

（二）安全事件监测情况

共监测发现11个网站被恶意篡改，主要集中在市级政府部门网站，篡改主要分为页面篡改和暗链两种形式，其中8个网站被黑客攻击，将网站页面指向博彩网站；3个网站被黑客插入了隐形恶意链接，链接主要为广告、博彩等网站，对政府网站形象造成了严重影响。

（三）安全漏洞检测情况

共监测发现存在高危漏洞网站50个，主要集中在市级以下政府、事业单位网站，漏洞类型主要为XSS攻击、SQL注入、OpenSSL POODLE、信息泄露等。

二、安全防御情况分析

（一）攻击源分析

经分析统计，网站攻击的IP总数为5878个，其中，境外IP数239个，境内IP数5639个。

从攻击源IP分布情况看，目前境外IP主要集中在保加利亚、俄罗斯、美国、日本、韩国等国家和地区（如图1），境内IP主要集中在江苏、浙江、上海、北京、湖北和陕西等（如图2）。

图1 境外攻击源分布情况

图2境内攻击源分布情况

（二）攻击类型分析

经分析统计，网站攻击最常见的攻击类型为恶意扫描和CC攻击。攻击者共发起了287.7776万次恶意扫描和61.2028万次CC攻击，所有攻击类型及数量的主要分布情况如图3。

图3网站恶意攻击类型及数量分布

三、威胁播报

（一）远程桌面协议出现 CredSSP 漏洞，影响所有版本的 Windows

RDP和WInRM中使用的CredSSP协议（安全加密Windows 用户远程登录过程）中出现严重漏洞，影响所有版本的 Windows。远程攻击者可以利用这个漏洞，使用RDP和WinRM 窃取数据并运行恶意代码。该漏洞编号为CVE-2018-0886，是一个逻辑加密漏洞，可被中间人攻击者利用，通过WiFi 或物理接触网络来窃取session认证数据，发起远程进程调用攻击。

如果用户和服务器通过RDP和WinRM连接协议进行认证，中间人攻击就能执行远程命令，入侵企业网络。而由RDP是远程登录中最常用的应用，几乎所有企业用户都在使用，因此，这个漏洞可造成大范围影响。目前，微软已经发布相关更新补丁，用户应尽快下载更新，同时可以禁用RDP等相关应用端口，尽可能少使用特权账户，多使用非特权账户。[文章来源：TheHackerNews]

（二）思科软件上的硬编码密码让攻击者能够接管linux服务器

Cisco Prime Collaboration Provisioning软件中发现了一个中等级别的漏洞，该漏洞可能允许本地攻击者将权限提升到root并完全控制系统。Cisco Prime Collaboration Provisioning（PCP）应用程序允许管理员远程控制公司内部署的思科通信设备（集成IP电话，视频，语音邮件）以及其服务的安装和管理。

这个漏洞（CVE-2018-0141）是因SSH的硬编码密码造成的，该密码可能被本地攻击者利用来连接PCP的Linux操作系统并获得权限。[文章来源：TheHackerNews]

（三）黑客可利用Windows远程协助窃取敏感文件

Trend Micro 0-day计划的研究人员发现微软的 Windows远程协助（快速访问）功能出现严重的信息披露漏洞（CVE-2018-0878），影响目前为止所有版本的Windows，Windows10、8.1、RT 8.1以及 7 都包括在内。利用这个漏洞，远程攻击者可以窃取目标计算机中的敏感文件。[文章来源：TheHackerNews]

（四）Sublime、Vim 等多款流行文本编辑器存在特权升级漏洞

据外媒3月16日报道，在最近一系列利用漏洞插件的攻击之后，SafeBreach的研究人员探讨了具有第三方可扩展性机制的高级文本编辑器如何被滥用来提升设备权限，并针对 Unix和Linux系统检查了几种流行的可扩展文本编辑器（Sublime、Vim、Emacs、Gedit、pico/nano）。经过研究发现，除pico/nano之外，所有受检查的编辑器都受到了一个关键的特权升级漏洞影响，攻击者可以利用这个漏洞在运行易受攻击的文本编辑器的目标设备上运行恶意代码。

据悉，大多数现代文本编辑器允许用户通过使用第三方插件来扩展功能，以此其增大攻击面。 研究人员认为这种情况非常严重，因为第三方插件可能会受到关键的特权升级漏洞影响，波及到类似WordPress、Windows的 Chrome、Firefox以及 Photoshop 等流行软件的插件。[文章来源：Security Affairs]

四、联系我们

欢迎与我们就《网络安全监测工作动态》进行交流。

本期编辑：王楠、赵少飞

联系电话：029-88319550-8017、8019

邮箱地址: wangnan@sntec.org.cn

网 址：<http://www.sntec.org.cn>