密级	公开

CVE-2015-3306 漏洞 全球预警报告 v1

[第一版 2015/04/23 下午]

北京知道创宇信息技术有限公司

监控预警中心 & ZoomEye

2015-04-23

1. 更新情况

版本	时间	描述
第一版	2015-04-23 14:30	第一版完成

2. 漏洞概要

2.1 漏洞信息

近日，开源 FTP 服务器程序 ProFTPd 被曝出一个未授权文件复制漏洞（CVE-2015-3306），该漏洞是由于 ProFTPd 中的 mod_copy 模块造成的。攻击者在一定条件下可利用该漏洞直接获得服务器权限。通过网络空间搜索引擎 ZoomEye 进行全网搜索，发现 ProFTPd 在全球网络空间中被普遍使用，该漏洞对欧美国家的服务器影响较大，中国受影响服务器的数量较少。

2.2 漏洞描述

ProFTPd 的 mod_copy 模块本用于文件复制操作，但在存在漏洞的版本中，mod_copy 模块的相关命令操作未设置访问授权验证，导致任意客户端均能通过特定命令对系统中任意文件进行复制，在一定条件下攻击者能够利用该漏洞获取系统敏感文件、获取服务器权限等。

目前，在许多 Linux 发行版（如 Debian）的软件包中，ProFTPd 都被默认安装并加载了存在该漏洞的 mod_copy 模块，直接对系统构成威胁。

2.3 漏洞影响

- 所有使用 ProFTPd 的服务器。

2.4 修复方案

目前 ProFTPd 官网（http://www.proftpd.org）提供下载的版本中并未修复该漏洞，但在开发版本（https://github.com/proftpd/proftpd/）中修复了该漏洞（增加了授权验证）。因此目前临时修复该漏洞的方法有两种：

第一， 从 https://github.com/proftpd/proftpd/ 上克隆最新源代码，重新编译安装；

第二， 暂时停用 mod_copy 模块，将 /etc/proftpd/modules.conf 配置文件中 LoadModule mod_copy.c 一行更改为 #LoadModule mod_copy.c，并重启 ProFTPd 服务。

3. ZoomEye 应急概要

3.1 全球受漏洞影响服务器分布

知道创宇安全研究团队通过网络空间搜索引擎 ZoomEye 进行全网搜索，得出目前全球 1,223,131 台设备中受 ProFTPd 漏洞影响的服务器有 57,445 台，占比 4.7%。

3.1.1 受漏洞影响服务器数量全球排名 TOP 10

受该漏洞影响的服务器数量全球排名前三分别是：德国 15,966 台（占全球受影响服务器比例 27.8%）、美国 10,995 台（占比 19.1%）以及法国 5,479 台（占比 9.5%）。中国受影响服务器共有 109 台（占比 0.2%）， 全球排名第 34 位。

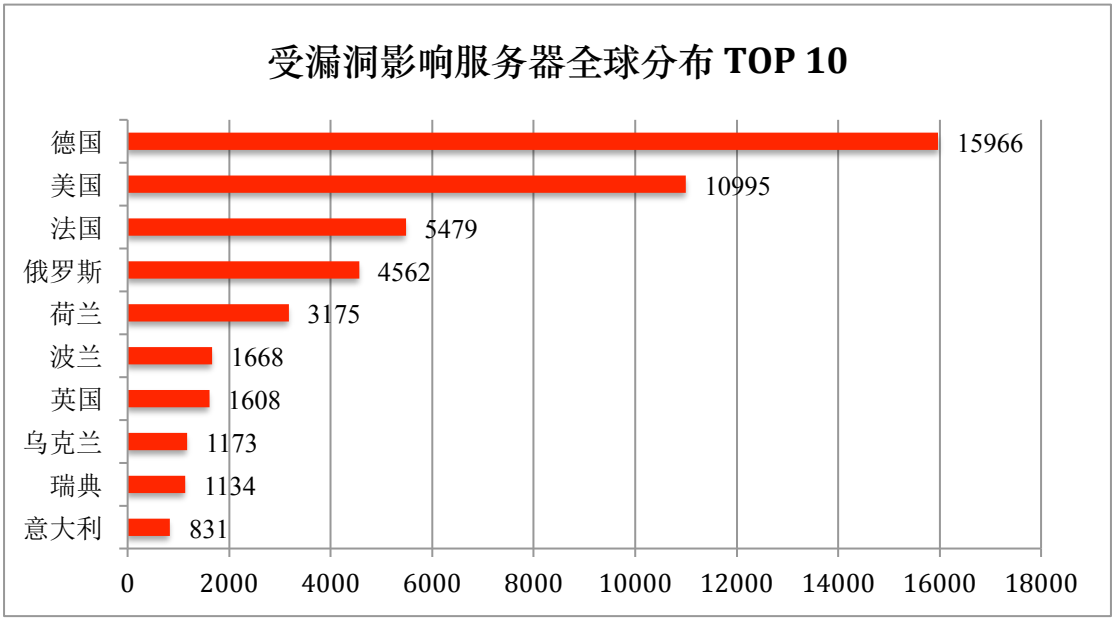

图 1 受漏洞影响服务器数量全球分布 TOP 10

3.1.2 受漏洞影响服务器所属厂商 TOP 10

如图 2 所示，受漏洞影响服务器所属公司/组织中 HetznerOnlineAG 有 4,561 台（7.94%）、OVHSAS 有 2,747 台（4.78%）、Savvis 有 1,994 台（3.47%）。其中，美国最大的网络电子商务公司亚马逊使用的服务器也被检测出有 1,670 台存在该漏洞，占比 2.9%，全球排名第四位。

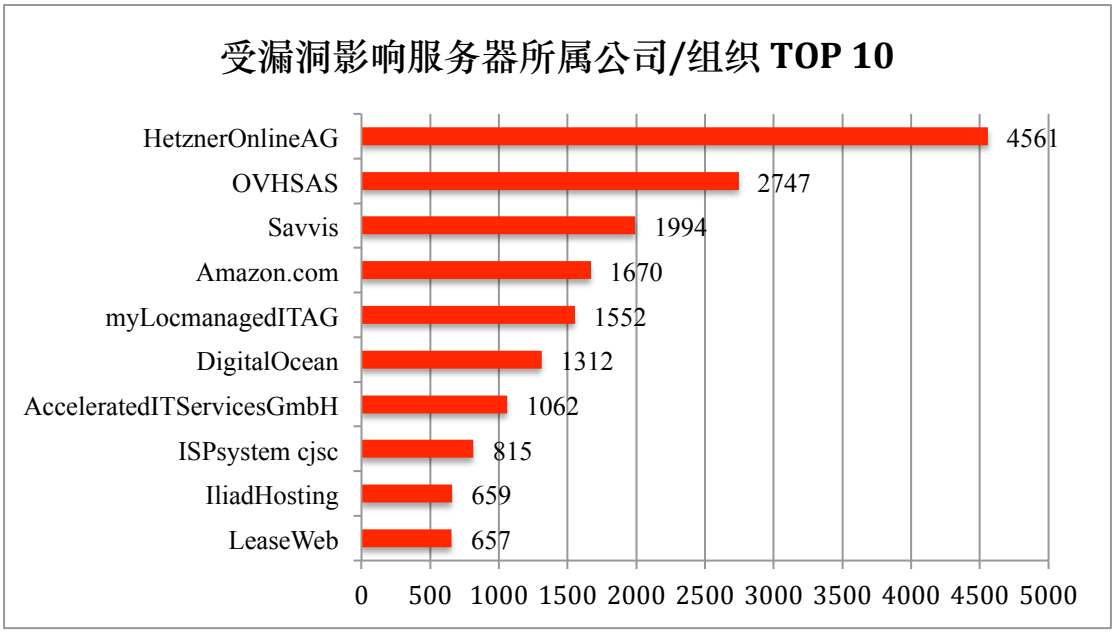

图 2 受漏洞影响服务器所属公司/组织 TOP 10

3.1.3 全球受漏洞影响的互联网服务提供商分布 TOP 10

全球主要受漏洞影响的互联网服务提供商分布如图 3 所示。

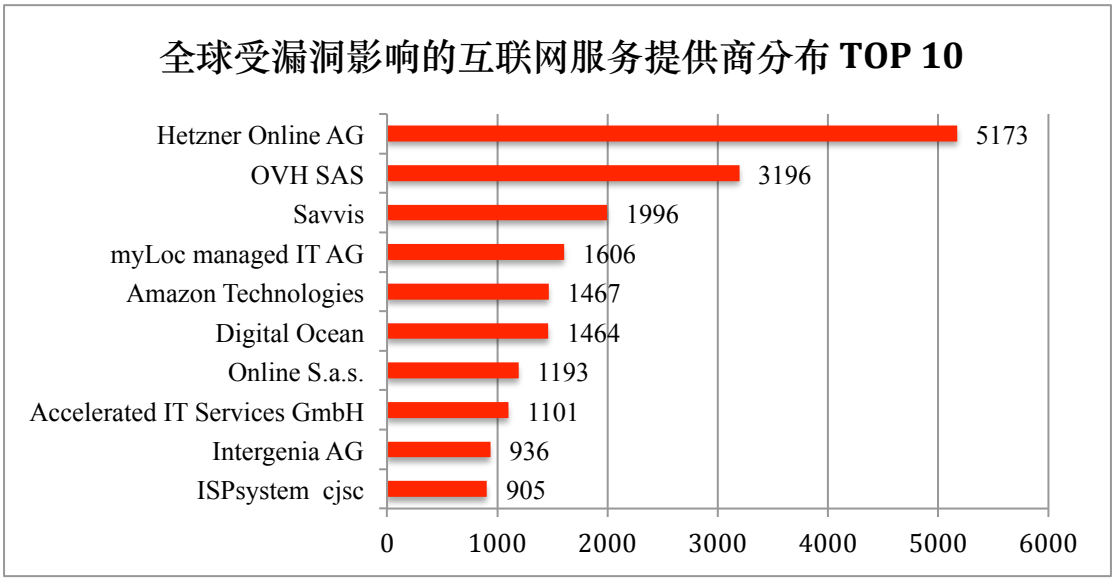

图 3 全球受漏洞影响的互联网服务提供商分布 TOP 10

3.1.4 全球受漏洞影响服务器地理分布

全球主要受漏洞影响服务器地理分布如图 4 所示。

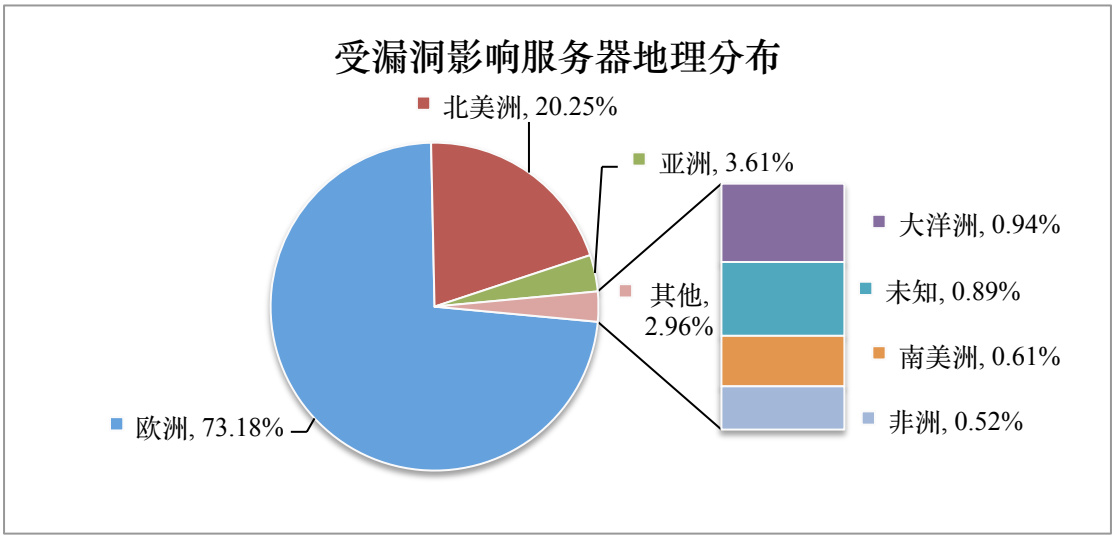

图 4 受漏洞影响服务器地理分布比例