2014

PC SECURITY LABS

Windows XP Operation System

Exploit Test

Microsoft Office

COMPARATIVES

PPStream

GLItemCom.DLL

Internet Explorer

Thunder

PCSL

IT CONSULTING INSTITUTE

目录

1. 测试背景

2001 年 10 月微软发布视窗操作系统 Windows XP，十余载后微软此前宣布对 Windows XP 的支持在 2014 年 4 月 8 日结束。随着科技发展的日新月异，云计算、移动、社交、大数据等新兴信息技术的快速发展， Windows XP 已经很难满足用户的需求，也不足以应对当前的网络安全威胁。由于微软官方对 Windows XP 的技术支持已经停止，Windows XP 将面临着各种已知或未知的漏洞攻击引起的危险。为此我们推出漏洞测试来测试各种安全软件对于已知漏洞的防护能力，以确保安全软件能更有效地对电脑进行保护。

漏洞是指一个系统存在的弱点或缺陷，系统对特定威胁攻击或危险事件的敏感性，或进行攻击的威胁作用的可能性。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意或无意地利用，从而对一个组织的资产或运行造成不利影响，如信息系统被攻击或控制，重要资料被窃取，用户数据被篡改，系统被作为入侵其他主机系统的跳板。

本次测试选用 Windows XP 作为靶机验证各安全软件对漏洞的防护能力。本次测试仅对是否防护漏洞执行成功进行评价，不代表最终防护能力。

2. 测试说明

判断防护是否成功的标准为

1. 安全产品导致漏洞触发无法成功视为防护成功，若触发成功则视为失败。
   如 Shellcode 成功执行视为防护失败。如文件监控干扰漏洞防护测试，则关闭文件监控。
   如被测产品使用强制重启，蓝屏等方式导致漏洞触发失败的，视为防护成功。
2. 本次测试环境仅限于 Windows XP，由于漏洞触发条件的不同，故不保证为 Windows XP 中某一个具体的版本。
3. 测试使用软件均由官网下载并安装。

3. 待测软件信息

软件名称	厂商	版本号
avast! Internet Security	AVAST	2014.9.0.2018
Avira Internet Security	Avira	14.0.3.350
百度卫士	Baidu	2.3.0.2224
Bitdefender Internet Security	Bitdefender	17.28.0.1191
ESET Smart Security	ESET	7.0.317.4
卡巴斯基反病毒软件	Kaspersky Lab	14.0.0.4651(g)
360安全卫士	Qihoo360	9.7.0.1002
Norton Internet Security	Symantec	21.3.0.12
电脑管家	Tencent	8.12

4. 测试结果

环境及漏洞名称	Qihoo360	Baidu	Avira	Bitdefender	Kaspersky
Windows XP SP3+IE8+Office2003	√	√	√	√	√
CVE-2009-3129(ms09_067) POC-A	pass	failed	failed	failed	failed
CVE-2010-0483 POC-A	pass	failed	failed	pass	failed
CVE-2010-2568(lnk) POC-A	failed	failed	failed	failed	failed
CVE-2012-0158 POC-A	pass	failed	failed	failed	some
CVE-2012-1875(ms12_037) POC-A	pass	failed	failed	failed	some
CVE-2012-4792 POC-A	pass	failed	failed	failed	some
CVE-2012-4969 POC-A	pass	failed	failed	some	some
CVE-2013-0810(主题) POC-A	failed	failed	failed	failed	failed
CVE-2013-3897 POC-A	pass	failed	failed	some	some
CVE-2009-3129(ms09_067) POC-B	pass	failed	failed	failed	some
CVE-2012-0158 POC-B	pass	failed	failed	failed	some
CVE-2012-4792 POC-B	pass	failed	failed	failed	some
CVE-2012-4969 POC-B	pass	failed	some	some	some
CVE-2013-0810（主题） POC-B	failed	failed	failed	failed	failed
CVE-2013-3897 POC-B	pass	failed	some	failed	some
CVE-2013-3163(MS13-055) POC-A	pass	failed	failed	failed	failed
CVE-2013-3918(MS13-090) POC-A	pass	failed	failed	failed	some
备注 如无特殊说明，统一关闭安全产品中的文件防护功能（若文件防护功能中包含网页流量监控则对文件防护功能设置排除后保持文件防护打开的状态）。 若产品包括网页监控（网页防护）功能保持此功能打开，若最终判定拦截是通过特征库进行识别拦截或者判定是通过主动防御等模块进行拦截，则判定为some。若同一漏洞的变种未能拦截，也判定为some。 如涉及到浏览器的漏洞，均为浏览器先运行本地文件进行触发，如拦截失败则本地新建服务器进行触发。		需要单独安装 XP 保护模块，本次测试已安装打开	Avira 的 web 防护会弹出检测框（如果选择拒绝页面强制跳转无法执行到 poc 故选择忽略），选择忽略后漏洞触发成功，视为 some。此外部分漏洞（如 CVE-2013-3897）会弹出多个框第一次没有选择拒绝后续及时拒绝仍能触发成功。	因为文件监控中带有 HTTP 流量扫描功能，故排除测试文件后保持文件监控打开状态	CVE-2009-3129，CVE-2012-0158 触发时拦截信息为 PDM:Exploit.Win32.Generic。PDM 为主动防御，实质上 shellcode 执行成功，故记为 some。 测试时关闭文件反病毒功能 网页反病毒功能给出警告 HEUR:Exploit.Script.Generic，认为网页反病毒是基于特征码检测统一记为 some。

环境及漏洞名称	Tencent	AVAST	ESET	Symantec
Windows XP SP3+IE8+Office2003	√	√	√	
CVE-2009-3129(ms09_067) POC-A	pass	failed	failed	failed
CVE-2010-0483 POC-A	pass	failed	failed	failed
CVE-2010-2568(lnk) POC-A	pass	failed	failed	failed
CVE-2012-0158 POC-A	pass	failed	failed	failed
CVE-2012-1875(ms12_037) POC-A	pass	pass	failed	some
CVE-2012-4792 POC-A	pass	pass	some	failed
CVE-2012-4969 POC-A	pass	pass	failed	failed
CVE-2013-0810(主题) POC-A	pass	failed	failed	failed
CVE-2013-3897 POC-A	pass	pass	failed	some
CVE-2009-3129(ms09_067) POC-B	pass	failed	failed	failed
CVE-2012-0158 POC-B	pass	failed	failed	failed
CVE-2012-4792 POC-B	pass	some	failed	pass
CVE-2012-4969 POC-B	pass	pass	some	pass
CVE-2013-0810（主题） POC-B	pass	failed	failed	failed
CVE-2013-3897 POC-B	pass	pass	some	pass
CVE-2013-3163(MS13-055) POC-A	pass	pass	pass	pass
	pass	failed	some	pass
备注 如无特殊说明，统一关闭安全产品中的文件防护功能（若文件防护功能中包含网页流量监控则对文件防护功能设置排除后保持文件防护打开的状态）。 若产品包括网页监控（网页防护）功能保持此功能打开，若最终判定拦截是通过特征库进行识别拦截或者判定是通过主动防御等模块进行拦截，则判定为 some。若同一漏洞的变种未能拦截，也判定为 some。 如涉及到浏览器的漏洞，均为浏览器先运行本地文件进行触发，如拦截失败则本地新建服务器进行触发。				CVE-2012-1875 本地双击无法触发成功，构建服务器后成功触发

结果小结

厂商	Tencent	Qihoo360	AVAST	Symantec	Kaspersky	ESET	Bitdefender	Avira	Baidu
拦截 Pass	17	14	7	5	0	1	1	0	0
部分拦截 Some	0	0	1	2	11	4	3	2	0
未拦截 Failed	0	3	9	10	6	12	13	15	17
总分	100.00	82.35	44.12	35.29	32.35	17.65	14.71	5.88	0.00

由于本次测试选取了 12 个漏洞及 17 个相关 POC，则成功拦截一个漏洞可获得 5.882 分，部分拦截加权为 2.941 分，未拦截不得分，最后相加获得实际总分。

5. 测试方简介

PC 安全实验室（简称：PCSL）成立于 2008 年 3 月，是一个致力于安全软件测试和相关测试标准研发的中立测评机构，并已加入国际反恶意软件测试标准组织 AMTSO 和亚洲反病毒研究者协会 AVAR 成为独立会员。PCSL 主办方为辰翔信息科技有限公司，位于浙江省嘉兴市。作为一家专业的计算机安全软硬件及 IT 软硬件的咨询测试公司，为用户选择 IT 产品提供参考。公司将在传统的 PC 端安全软件咨询测试的基础上逐步开展 PC 端通用软件、服务器安全软件及其他通用软硬件的咨询与测试工作。

联系地址：浙江省嘉兴市南湖区凌公塘路 3339 号科创中心 3 号楼 3304-3306

TEL: +86 573 82809089 FAX: +86 573 82808561 Mail：info@pitci.com

6. 权利说明

7. 免责声明

辰翔科技在此特别提醒，在使用本公司报告前，请认真阅读、充分理解本声明中各条款，包括免除或限制辰翔科技责任的免责条款及对用户的权利限制，如果您对本声明中的任何条款表示异议，可以选择不使用本报告，您使用本报告的行为将被视为对本声明全部内容的认可，并同意接受本声明全部条款的约束。

1、本报告由辰翔科技向读者提供，所载全部内容仅系提供读者参考之用，并不构成对其选择、购买、使用产品之建议，也不构成对其选择、购买、使用报告中所涉产品的邀请或保证。辰翔科技不担保内容的绝对准确性和完整性，读者不应单纯依靠本报告而取代个人的独立判断，辰翔科技建议读者如有任何疑问，应当咨询国家相关部门并进行独立选择、购买或使用判断。

2、本报告所载内容为辰翔科技在报告发表日当日对有关产品性状的判断，在其它不同日期辰翔科技可发出与本报告内容不一致或有不同结论的报告，但辰翔科技无义务或责任为此将原报告涉及内容及时更新并由此通知读者，在此情形下辰翔科技不对读者因使用本报告所产生的损失负任何责任。

3、 本报告可能附带其它网站的地址或超级链接，目的纯粹是为了读者使用方便，所链接网站的内容不构成本报告的任何部分，读者需自行承担浏览该类网站的风险、费用或者损失。同时辰翔科技不对此类网站的内容（包括但不限于广告、产品或其他资料）的真实性、完整性、准确性及合法性负责或保证，读者使用或依赖任何此类网站或经由此类网站获得的任何内容、商品或服务所产生的任何损害或损失，辰翔科技不承担任何直接或间接法律责任。

4、辰翔科技可能与生产本报告涉及产品的公司间已存在或将存在业务关系，但无需事先或在将来建立业务关系后通知其他读者。

5、读者接收本报告并不视为和辰翔科技建立业务关系，辰翔科技无需因此而对其承担类似客户关系情形下的任何法律责任。

6、所有辰翔科技报告测试对象之产品样品，系辰翔科技于正规合法销售渠道购买之产品，故本报告内容仅适合于从正规合法渠道购买之产品，而不适于从其他渠道所得之产品，读者使用非正规合法销售渠道产品所产生的任何风险或损失，与辰翔科技无关，在此情形下辰翔科技概不承担任何法律责任。

7、本报告可能会涉及公司或个人所有的商标或其相关照片、图案，若任何单位或个人认为涉嫌侵犯其合法权益，可及时与辰翔科技联系，以便辰翔科技迅速作出处理。

对上述声明的解释、修改及更新权属辰翔科技所有。

Notice that before using the report issued by Jiaxing Chenxiang Information Technology Co. Ltd (hereinafter referred to as "Chenxiang Information Technology") , please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as "Disclaimer "), including the clauses of exclusion or restriction of the liabilities of Chenxiang Information Technology and the limitation the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as an acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1、The report is provided by Chenxiang Information Technology, all the contents contained herein are for reference purpose only, but will not be regarded as the suggestion, invitation or warranty for readers to choose, purchase or use the products mentioned herein. Chenxiang Information Technology will not guarantee the absolute accuracy and completeness of the contents of the report, you should not rely solely on this report or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State and then choose, purchase or use products by your independent judgment.

2、The contents contained herein is the judgment made by Chenxiang Information Technology to the product characteristics as of the date of the report published, in the future Chenxiang Information Technology will have the right to issue the new reports which contain different contents or draw different conclusions, but Chenxiang Information Technology has no obligation or responsibility to update the original report or inform readers of the update of it, in this case, Chenxiang Information Technology will bear no responsibility for readers' loss of using the original report .

3、The report may contain links to other websites, which are provided solely for readers' convenience to use, the contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites, Chenxiang Information Technology will not guarantee the authenticity, completeness , accuracy and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). Chenxiang Information Technology does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products or service.

4、Chenxiang Information Technology may have or will have a business relationship with the companies which produce the products mentioned in this report, but has no obligation to notify readers about it, no matter there has already been or there will be such business relationship in the future.
5、The act of readers' receiving this report are not regarded as the establishment of the business relationship between readers and Chenxiang Information Technology, so there is no customer relationship existing, Chenxiang Information Technology does not accept any legal liability as the readers' customer .
6、The products which are used to be tested as the samples by Chenxiang Information Technology are bought through official way and legal means, so the report is proper for products bought through official way and legal means, not for products bought through unofficial way and illegal means. Therefore it' s the users buying such products who will be responsible for any risk or loss arising therefrom. Chenxiang Information Technology will not have or accept any liability whatsoever for any such risk or loss.
7、Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact Chenxiang Information Technology promptly, Chenxiang Information Technology will handle the matter as quickly as possible.
Chenxiang Information Technology reserves the rights to interpret, modify and update the Disclaimer.