Security Software Evaluation

17 April 2014

CONFIDENTIAL

Contents

1. Executive summary 3
1.1. Overview 3
1.2. Scope of work 3
1.3. Methodology 3
1.4. Test Environment 4
1.5. List of Security Software 4
1.6. List of CVEs 5
1.6.1. CVEs related to Internet Explorer 8 5
1.6.2. CVEs related to Windows XP Kernel 5
1.6.3. CVEs relate to Microsoft Office 2003 5
1.7. Findings Summary 6
1.8. Conclusion and Recommendations 7
2. Technical Details 8
2.1. Table on Findings 8
2.1.1. IE8 Vulnerabilities 8
2.1.2. Windows XP Kernel Vulnerabilities 9
2.1.3. Microsoft Office 2003 Vulnerabilities 10
3. Additional Details 11
3.1. Warning box from Kaspersky 11

1. Executive summary

COSEINC was engaged to perform a security software evaluation. The aim is to determine if known security exploits can still execute on Windows XP when the operating system is protected by the security software of interest.

1.1.Overview

Windows XP and Microsoft Office 2003 will enter its end-of-support on 8 April 2014. This implies that no further security patches for these 2 products will be release after this date and this puts millions of computers that are still running Windows XP at security risk.

COSEINC was tasked to evaluate the effectiveness of Windows XP security protection by some of the leading security vendors in the market.

1.2.Scope of work

The objective of this test is for COSEINC to undertake the role of an independent assessor and determine the extent of protection a security software can offer under windows XP. This is a blackbox testing with no knowledge on the internal workings of the security software.

1.3.Methodology

Our methodology follows closely to our internally developed security software testing framework.

This includes the following phases

- Information Gathering
- Environment Preparation
- Testing & Repeatability Testing
- Observation and Recording
- Documentation

During testing, one important benchmark is on shellcode execution. We will be closely monitoring this and will classify each exploit under one of the following

- The shellcode did not execute – protection is successful
- The shellcode executes, but failed to start any process or download from the internet – partial protection enforced
- The shellcode or payload executes, but stealing of files failed – partial protection enforced
- All other cases will be classified as unsuccessful protection.

1.4.Test Environment

The test environment was setup as a guest virtual machine running under QEMU 1.7.0.

Within the guest virtual machine, the following operating system and software are installed:

- Microsoft Windows XP Professional Service Pack 3 – 5.1.2600.5512
- Internet Explorer – 8.0.6001.18702
- Microsoft Office 2003 Professional Edition
  - Word – 11.8322.5606
  - Excel – 11.5612.5606

1.5.List of Security Software

The following is the list of security software that we will be testing on. For each vendor, we will only be testing on the latest version of one product that can install on Windows XP. The software are

- AVAST Free Antivirus – 2014.9.0.2013
- AVG Antivirus Free – 2014.0.4336
- Avira Free Antivirus – 14.0.3.350
- BitDefender Antivirus Plus – 17.26.0.1106
- Kaspersky Pure 3.0 Trial – 13.0.2.558
- Kingsoft DUBA – SP7
- Qihoo 360 AnQuanWeiShi– 9.7.0.1001
- Tencent QQ Doctor – 8.9.10958.231

1.6. List of CVEs

We have used known CVEs to determine if an exploitation is successful. The list of CVEs that were used in the testing are as follows,

1.6.1. CVEs related to Internet Explorer 8

- CVE-2009-1141
- CVE-2009-1136
- CVE-2012-1875
- CVE-2013-1347
- CVE-2013-3163

1.6.2. CVEs related to Windows XP Kernel

- CVE-2010-0233
- CVE-2010-1897
- CVE-2011-2005
- CVE-2012-2529
- CVE-2013-3660
- CVE-2013-5065

1.6.3. CVEs relate to Microsoft Office 2003

- CVE-2009-1129
- CVE-2009-3129
- CVE-2011-1990
- CVE-2012-0158

1.7.Findings Summary

This section summarises the key findings of the security software evaluation. Details from the test can be obtained from section 2.1.

As a summary, testing of the 8 security software was conducting using 3 categories of known exploits, with 5 exploits targeting Internet Explorer 8, 6 exploits targeting Windows XP kernel and 4 exploits targeting Microsoft Office 2003.

For the Internet Explorer 8 category, Qihoo 360 AnQuanWeiShi is the only security software that managed to stop all exploits in this category. The rest of the security software failed to stop one or more exploits.

Next, in the Windows XP kernel category, Qihoo 360 AnQuanWeiShi is again the only security software that managed to stop all exploits used in the test.

Lastly, for the Microsoft Office 2003 category, Avira Free Antivirus, Kaspersky Pure 3.0 Trial and Qihoo 360 AnQuanWeiShi managed to stop all the tested exploits, with the rest of the security software failing to prevent one or more exploits from running.

When taking all 3 categories into consideration, it is evident that only Qihoo 360 AnQuanWeiShi stopped all known exploits in every tested category. As such, Qihoo 360 AnQuanWeiShi offers the most protection for Windows XP and Microsoft Office 2003.

Summary table of the finding is as follows,

CVEs	Avast	AVG	Avira	Bitdefender	Kaspersky	Kingsoft	Qihoo	Tencent
Number of CVEs successfully protected against	9	11	12	8	11	5	15	5
Number of CVEs failed to protect against	6	4	3	7	3	10	0	10
Number of CVEs that were displayed as warning*	0	0	0	0	1	0	0	0

* A warning box pops out, stating that sample lacks digital signature, but it did not indicate that the sample is malicious. Refer to section 3.1 for details.

Based on the summary table of findings, the security software were ranked with respect to the percentage of test exploits that were successfully blocked.

Below is the ranking table,

Vendor	Percentage of test exploits that were successfully blocked
Qihoo	100%
Avira	80%
AVG	73%
Kaspersky	73%
Avast	60%
Bitdefender	53%
Kingsoft	33%
Tencent	33%

1.8.Conclusion and Recommendations

Having completed the security software evaluation, COSEINC felt that the security software by Qihoo 360 AnQuanWeiShi offers the most protection for Windows XP when tested against the list of known exploits. COSEINC would recommend users to install this software on their Windows XP machines to protect themselves, as Microsoft no longer provides security updates to Windows XP and Office 2003.

2. Technical Details

2.1.Table on Findings

The tables in this section show the results of the test.

2.1.1. IE8 Vulnerabilities

CVE	Result	Avast	AVG	Avira	Bitdefender	Kaspersky	Kingsoft	Qihoo	Tencent
CVE-2009-1141	Creates another process	Protected	Protected	Protected	Protected	Protected	Protected	Protected	Protected
CVE-2009-1136	Crashes IE	Protected	Protected	Failed	Failed	Protected	Protected	Protected	Failed, but some popup comes up asking to try to fix it
CVE-2012-1875	Crashes IE	Protected	Protected	Protected	Protected	Protected	Protected	Protected	Protected
CVE-2013-1347	Launches cmd.exe	Failed	Protected	Protected	Protected	Protected	Failed	Protected	Failed
CVE-2013-3163	Crashes IE	Protected	Failed	Failed	Failed	Failed	Failed	Protected	Failed

CONFIDENTIAL

2.1.2. Windows XP Kernel Vulnerabilities

CVE	Result	Avast	AVG	Avira	Bitdefender	Kaspersky	Kingsoft	Qihoo	Tencent
CVE-2010-0233	Spawns shell with SYSTEM privileges	Protected	Protected	Protected	Protected	Protected	Failed	Protected	Failed
CVE-2010-1897	Spawns shell with SYSTEM privileges	Failed	Protected	Protected	Protected	Failed	Failed	Protected	Failed
CVE-2011-2005	Spawns shell with SYSTEM privileges	Failed	Failed	Protected	Failed	Warning only	Failed	Protected	Failed
CVE-2012-2529	Creates process	Failed	Protected	Protected	Failed	Protected	Protected	Protected	Failed
CVE-2013-3660	Spawns shell with SYSTEM privileges	Protected	Protected	Protected	Failed	Protected	Failed	Protected	Failed
CVE-2013-5065	Launches process with SYSTEM privileges.	Failed	Failed	Failed	Protected	Failed	Protected	Protected	Protected

CONFIDENTIAL

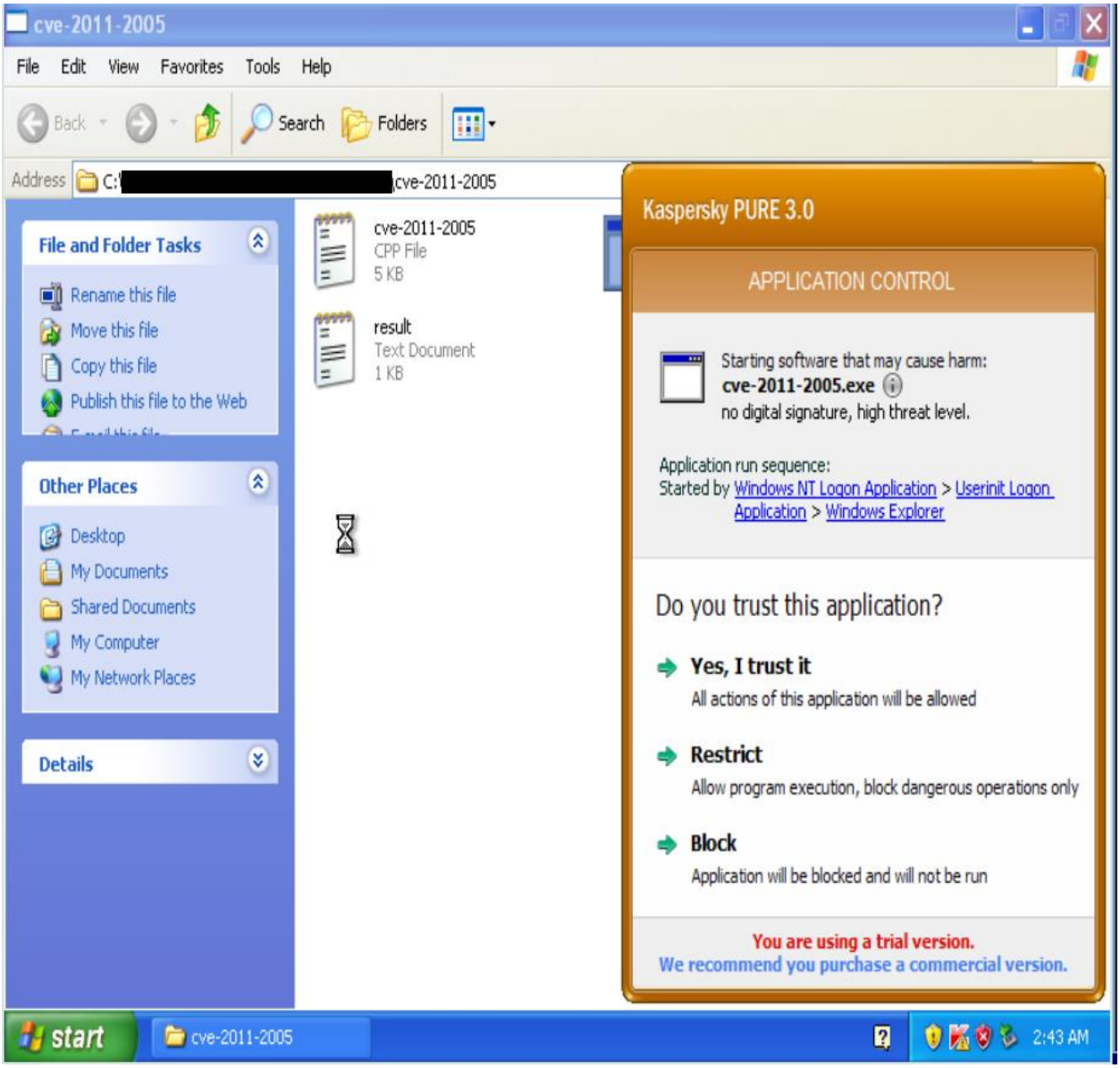
2.1.3. Microsoft Office 2003 Vulnerabilities

CVE	Result	Avast	AVG	Avira	Bitdefender	Kaspersky	Kingsoft	Qihoo	Tencent
CVE-2009-1129	Spawns shell with USER privileges	Protected	Failed	Protected	Failed	Protected	Failed	Protected	Protected
CVE-2009-3129	Spawns shell with USER privileges	Protected	Protected	Protected	Failed	Protected	Failed	Protected	Failed
CVE-2011-1990	Launches an app.exe	Protected	Protected	Protected	Protected	Protected	Failed	Protected	Protected
CVE-2012-0158	Launches calculator	Failed	Protected	Protected	Protected	Protected	Failed	Protected	Failed

3. Additional Details

3.1. Warning box from Kaspersky

Here is a screenshot of the warning box when testing CVE-2011-2005 on Kaspersky Pure 3.0 Trial. It showed that the CVE was detected because it lacked a digital signature, and not because it was malicious.



CONFIDENTIAL