Internet Security Suite test October 2008

Introduction

Secunia has tested the ability of various high-profile Internet Security Suites to detect exploitation of vulnerabilities.

For a long time, we have been quite convinced that *anti-virus* products would exhibit poor performance in this discipline, given the name “anti-virus” which suggests a limited focus (though customers may still expect to be protected).

This is why we decided to test some more “high-end” product bundles that are being marketed as comprehensive Internet Security Suites, thus leaving the impression that the user is “fully protected against all Internet threats”.

Secunia decided to test the following twelve Internet Security Suites:

- McAfee Internet Security Suite 2009
- Norton Internet Security 2009
- Windows Live OneCare
- ZoneAlarm Security Suite 8
- AVG Internet Security 8.0
- CA Internet Security Suite 2008
- F-secure Internet Security 2009
- TrendMicro Internet Security 2008
- BitDefender Internet Security Suite 2009
- Panda Internet Security 2009
- Kaspersky Internet Security 2009
- Norman Security Suite 7.10

Exploits

As part of our Binary Analysis Service, we have developed hundreds of exploits for vulnerabilities in high-end or commonly used products. These exploits have all been developed in-house by Secunia based on the in-depth analysis of vulnerabilities and have been supplied to various security vendors over the last two years in order for them to test the performance of their own products.

The test cases are a mix of three different kinds of exploits:

- Proof of Concept (PoC) – The purpose of a PoC is to just trigger the vulnerability. It does not carry a payload. If a security product can reliably detect a PoC, then it can detect all attempts to exploit the vulnerability independent of the payload.
- GameOver PoC – The purpose of a GameOver PoC is to prove that code execution is possible by gaining control of the program flow, without actually launching any code.
- Exploit – Exploits carry a payload and will execute it if used against a vulnerable application.

In real life, an attacker would always use an exploit. However, if a security product can not detect a PoC it also can not detect an exploit reliably.

History

Historically, malware has been delivered as a file that could be executed on a system. This is what the anti-virus vendors need to analyse and make a signature of.

Browsers and e-mail clients usually warn the user when he/she tries to download or open such executable files e.g. most users have already learned not to open .exe, .scr, and other common, potentially dangerous file types.

However, when talking about vulnerabilities and exploits, it is no longer clear that the file is of a “dangerous” type. In fact, the file may be an innocent-looking .doc or .jpg file. When a specially crafted file is opened by a vulnerable program, it is possible to trigger the vulnerability and inject code into the program opening the file. From this point forward, an attacker literally has the same level of control of the computer as the user behind the keyboard.

Vulnerabilities may also be exploited in many other ways depending on the vulnerable program.

The test

All tests were carried out on Windows XP SP2 missing certain patches and with a number of vulnerable programs. ZoneAlarm was tested on an SP3 machine due to compatibility issues.

The test cases were separated into two groups:

1. The first group consisted of 144 malicious *files* (e.g. .gif, .bmp, .mov, and office documents).
2. The other group consisted of 156 malicious *web pages* triggering e.g. ActiveX and browser vulnerabilities.

The testing process consisted of the following steps:

1. The malicious files were first tested by unpacking a ZIP archive containing the files in order to test the efficiency of real-time access scanning.
2. Then the folder was scanned manually to ensure that all files were scanned, regardless of any policy limitations on the real-time scanning.
3. Malicious web pages were tested using Internet Explorer to visit the individual pages one by one. This was done using regular http connections to ensure that none of the products would be foiled by encrypted https traffic (even though a good product should not be affected by this).

Out of the 300 test cases, 126 are considered particularly important. These 126 test cases affect very popular products and have either been discovered as zero-day threats, public exploits exist, or Secunia has developed working exploits.

Note: Secunia does not usually develop working exploits as the Secunia Binary Analysis service is defensive in nature; thus working exploits are not necessary for developing and testing signatures. Generally speaking, Secunia focuses on developing PoCs for the analysed vulnerabilities, since these are better suited for signature development.

The results*

*Important threats emphasized in purple colour

SAID	CVE	Filename	McAfee	Norton	OneCare	ZoneAlarm	AVG	CA	F-Secure	TrendMicro	BitDefender	Panda	Kaspersky	Norman
SA14896	CVE-2005-0944	PoC.mdb		Found!										
SA20748#1	CVE-2006-3086	PoC.xls									Found!			
SA21061	CVE-2006-3655	POC1.ppt		Found!						Found!	Found!			
SA21061	CVE-2006-3656	POC2.ppt		Found!						Found!	Found!			
SA21061	CVE-2006-3660	POC3.ppt		Found!										
SA22127#1	CVE-2006-4694	PoC.ppt	Found!	Found!		Found!		Found!	Found!				Found!	
SA23540	CVE-2007-0015	PoC.qtl		Found!										
SA23676#2	CVE-2007-0028	Exploit1.xls												
SA23676#2	CVE-2007-0028	exploit2.xls												
SA23676#2	CVE-2007-0028	PoC.xls												
SA23676#3	CVE-2007-0029	PoC.xls												
SA23676#4	CVE-2007-0030	PoC.xls		Found!										
SA23676#5	CVE-2007-0031	PoC.xls		Found!										
SA24152	CVE-2006-1311	PoC.rtf		Found!										
SA24359#1	CVE-2007-0711	PoC.3gp												
SA24359#3	CVE-2007-0713	PoC.mov												
SA24359#4	CVE-2007-0714	PoC.mov												
SA24359#8	CVE-2007-0718	PoC.qtif												
SA24359#9	CVE-NOMATCH	PoC.jp2												
SA24659	CVE-2007-0038	GameOver.ani	Found!	Found!			Found!		Found!	Found!	Found!	Found!	Found!	
SA24664	CVE-2007-1735	PoC.wpd												
SA24725	CVE-2007-1867	GameOver.ani	Found!	Found!		Found!	Found!			Found!	Found!	Found!	Found!	
SA24784	CVE-2007-1942	Exploit.bmp												
SA24784	CVE-2007-1942	PoC.bmp												
SA24884	CVE-2007-2062	GameOver.cue												
SA24973	CVE-2007-2194	GameOver.xpm												
SA25023	CVE-2007-2244	PoC.bmp												
SA25034	CVE-2007-2366	GameOver.png												
SA25044	CVE-2007-2365	GameOver.png												
SA25052	CVE-2007-2363	GameOver.iff												
SA25089	CVE-2007-2498	PoC.mp4												
SA25150#1	CVE-2007-0215	PoC1.xls												
SA25150#1	CVE-2007-0215	PoC2.xls												
SA25150#3	CVE-2007-1214	PoC.xls		Found!										
SA25178	CVE-2007-1747	PoC.xls												
SA25278	CVE-2007-2809	GameOver.torrent												
SA25426	CVE-2007-2966	PoC.lzh												
SA25619#1	CVE-2007-0934	PoC.vsd												
SA25619#2	CVE-2007-0936	GameOver.vsd		Found!										
SA25619#2	CVE-2007-0936	PoC.vsd		Found!										
SA25826	CVE-2007-3375	PoC.lzh												
SA25952	CVE-2007-6007	PoC1.psp												
SA25952	CVE-2007-6007	PoC2.psp												
SA25952	CVE-2007-6007	PoC3.psp												
SA25988	CVE-2007-1754	PoC.pub		Found!										
SA25995#1	CVE-2007-1756	PoC.xls												
SA25995#2	CVE-2007-3029	PoC1.xls												
SA25995#2	CVE-2007-3029	PoC2.xls												
SA25995#3	CVE-2007-3030	PoC.xlw												
SA26034#4	CVE-2007-2394	PoC.mov												
SA26145	CVE-2007-3890	PoC1.xlw												
SA26145	CVE-2007-3890	PoC2.xlw												
SA26433	CVE-2007-3037	PoC.wmz												
SA26619	CVE-2007-4343	Exploit.pal												
SA26619	CVE-2007-4343	GameOver.pal												
SA27000	CVE-2007-5279	PoC.bh												
SA27151	CVE-2007-3899	GameOver.doc												
SA27151	CVE-2007-3899	PoC.doc												
SA27270	CVE-2007-5709	GameOver.m3u												
SA27304#1	CVE-2007-5909	GameOver1.rtf												
SA27304#1	CVE-2007-5909	GameOver2.rtf												
SA27304#1	CVE-2007-5909	PoC1.rtf												
SA27304#2	CVE-2007-6008	PoC1.eml												
SA27304#2	CVE-2007-6008	PoC2.eml												
SA27361#4	CVE-2007-2263	PoC.swf												

SAID	CVE	Filename	McAfee	Norton	OneCare	ZoneAlarm	AVG	CA	F-Secure	TrendMicro	BitDefender	Panda	Kaspersky	Norman
SA27849	CVE-2007-6593	GameOver1.123												
SA27849	CVE-2007-6593	GameOver2.123												
SA27849	CVE-2007-6593	GameOver3.123												
SA28034	CVE-2007-0064	PoC1.asf												
SA28034	CVE-2007-0064	PoC2.asf								Found!				
SA28034	CVE-2007-0064	PoC3.asf								Found!				
SA28034	CVE-2007-0064	PoC4.asf												
SA28083#2	CVE-2007-0071	PoC.swf	Found!	Found!							Found!			
SA28092#1	CVE-2007-4706	PoC.mov												
SA28209#10	CVE-2007-5399	PoC_bcc.eml												
SA28209#10	CVE-2007-5399	PoC_cc.eml												
SA28209#10	CVE-2007-5399	PoC_date.eml												
SA28209#10	CVE-2007-5399	PoC_from.eml												
SA28209#10	CVE-2007-5399	PoC_imp.eml												
SA28209#10	CVE-2007-5399	PoC_prio.eml												
SA28209#10	CVE-2007-5399	PoC_to.eml												
SA28209#10	CVE-2007-5399	PoC_xmsmail.eml												
SA28209#11	CVE-2007-5399	PoC.eml												
SA28209#12	CVE-2007-5399	PoC.eml												
SA28209#13	CVE-2007-5399	PoC.eml												
SA28326	CVE-2008-0064	GameOver1.hdr												
SA28326	CVE-2008-0064	GameOver2.hdr												
SA28506#1	CVE-2008-0081	Exploit.xls		Found!										
SA28506#1	CVE-2008-0081	PoC.xls		Found!										
SA28506#2	CVE-2008-0111	PoC1.xls		Found!										
SA28506#2	CVE-2008-0111	PoC2.xls		Found!										
SA28506#2	CVE-2008-0111	PoC3.xls												
SA28506#4	CVE-2008-0114	PoC.xls		Found!										
SA28506#7	CVE-2008-0117	Exploit.xls		Found!										
SA28506#7	CVE-2008-0117	GameOver.xls		Found!										
SA28506#7	CVE-2008-0117	PoC.xls												
SA28563	CVE-2008-0392	Exploit_CommandName.dsr												
SA28563	CVE-2008-0392	GameOver_CommandName.dsr												
SA28765	CVE-2008-0619	PoC.m3u												
SA28765	CVE-2008-0619	PoC.pls												
SA28802#1	CVE-2007-5659	GameOver.pdf												
SA28802#1	CVE-2007-5659	PoC.pdf												
SA28904#2	CVE-2008-0105	PoC1.wps									Found!			
SA28904#2	CVE-2008-0105	PoC2.wps												
SA28904#3	CVE-2007-0108	GameOver.wps												
SA29293#1	CVE-2008-1581	PoC.pct												
SA29321#2a	CVE-2008-0118	PoC.ppt												
SA29321#2b	CVE-2008-0118	GameOver.ppt												
SA29321#2b	CVE-2008-0118	PoC.ppt												
SA29620	CVE-2008-0069	GameOver.sld												
SA29650#5	CVE-2008-1017	crgn_PoC.mov												
SA29704#1	CVE-2008-1083	PoC.emf												
SA29704#2	CVE-2008-1087	PoC.emf										Found!		
SA29838	CVE-2008-1765	Exploit.bmp												
SA29838	CVE-2008-1765	GameOver.bmp												
SA29934	CVE-2008-1942	PoC_ExtGState.pdf												
SA29934	CVE-2008-1942	PoC_Height.pdf												
SA29934	CVE-2008-1942	PoC_MediaBox.pdf												
SA29934	CVE-2008-1942	PoC_Width.pdf												
SA29941	CVE-2008-1104	Exploit.pdf												
SA29941	CVE-2008-1104	PoC.pdf												
SA29972	CVE-2008-2021	PoC.ZOO												
SA30143#1	CVE-2008-1091	PoC.rtf												
SA30953	CVE-2008-1435	PoC.search-ms												
SA30975	CVE-2008-2244	PoC1.doc												
SA30975	CVE-2008-2244	PoC2.doc												
SA31336#2	CVE-2008-3018	PoC.pict												
SA31336#4	CVE-2008-3020	PoC.bmp												
SA31336#5	CVE-2008-3460	PoC1.wpg												
SA31336#5	CVE-2008-3460	PoC2.wpg												
SA31336#5	CVE-2008-3460	PoC3.wpg												
SA31385	CVE-2008-2245	PoC.emf												

SAID	CVE	Filename	McAfee	Norton	OneCare	ZoneAlarm	AVG	CA	F-Secure	TrendMicro	BitDefender	Panda	Kaspersky	Norman
SA31441	CVE-2008-4434	PoC.torrent												
SA31454#X	CVE-NOMATCH	PoC.xls												
SA31454#2	CVE-2008-3005	Exploit.xls												
SA31454#2	CVE-2008-3005	PoC.xls												
SA31675#3	CVE-2008-3013	PoC.gif												
SA31675#4	CVE-2008-3014	PoC.wmf												
SA31675#X	CVE-NOMATCH	PoC.emf												
SA31675#X	CVE-NOMATCH	PoC.wmf												
SA31675#5	CVE-2008-3015	PoC.ppt												
SA31821#6	CVE-2008-3626	PoC1.mp4												
SA31821#6	CVE-2008-3626	PoC2.mp4												
SA20807	CVE-2006-5579	PoC.html												
SA22251	CVE-2007-1559	Exploit1.html												
SA22251	CVE-2007-1559	PoC1.html												
SA22251	CVE-2007-1559	Exploit2.html												
SA22251	CVE-2007-1559	PoC2.html												
SA22603	CVE-2006-4704	Exploit.htm												
SA22896	CVE-2007-1205	PoC.html	Found!	Found!										
SA23032	CVE-2007-0348	Exploit.html												
SA23032	CVE-2007-0348	GameOver.html												
SA23043	CVE-2006-6442	Exploit.html		Found!										
SA23043	CVE-2006-6442	PoC.html		Found!										
SA23469	CVE-2007-3893	PoC.html												
SA23475	CVE-2007-0018	Exploit.html		Found!										
SA23475	CVE-2007-0018	PoC.html		Found!										
SA23583	CVE-2006-6488	Exploit2.html												
SA23583	CVE-2006-6488	PoC2.html												
SA23677#1	CVE-2007-0024	PoC.html		Found!										
SA23677#2	CVE-NOMATCH	PoC.html		Found!										
SA24170	CVE-2007-0979	Exploit.html												
SA24170	CVE-2007-0979	PoC.html												
SA24422	CVE-2007-1637	Connect_GameOver.html												
SA24422	CVE-2007-1637	Connect_PoC.html												
SA24422	CVE-2007-1637	WebConnect_GameOver.html												
SA24422	CVE-2007-1637	WebConnect_PoC.html												
SA24466	CVE-2007-1498	PoC1.html												
SA24466	CVE-2007-1498	PoC2.html												
SA24692	CVE-2007-1819	Exploit.html												
SA24692	CVE-2007-1819	PoC.html												
SA24710	CVE-2007-2323	gameover.html												
SA24710	CVE-2007-2323	PoC.html												
SA24714	CVE-2006-5820	Exploit.html												
SA24714	CVE-2006-5820	PoC.html												
SA25173	CVE-2007-2584	Exploit.html												
SA25173	CVE-2007-2584	GameOver.html												
SA25215	CVE-2007-2955	Exploit.html		Found!										
SA25215	CVE-2007-2955	GameOver.html		Found!										
SA25514_1	CVE-2007-2918	Exploit.html												
SA25514_1	CVE-2007-2918	GameOver.html		Found!										
SA25514_2	CVE-2007-2918	GameOver.html												
SA25514_3	CVE-2007-2918	Exploit2.html												
SA25514_3	CVE-2007-2918	PoC2.html												
SA25514_3	CVE-2007-2918	Exploit1.html												
SA25514_3	CVE-2007-2918	GameOver1.html												
SA25514_3	CVE-2007-2918	SetAdvisePresent_PoC.html												
SA25514_3	CVE-2007-2918	SetPicShareAdvise_PoC.html												
SA25514_4	CVE-2007-2918	Exploit.html												
SA25514_4	CVE-2007-2918	GameOver.html												
SA25514_4	CVE-2007-2918	RecvVideo_Exploit.html												
SA25514_4	CVE-2007-2918	RecvVideo_GameOver.html												
SA25514_4	CVE-2007-2918	RemoveImage_Exploit.html												
SA25514_4	CVE-2007-2918	RemoveImage_GameOver.html												
SA25514_4	CVE-2007-2918	SendCommand_Exploit.html												
SA25514_4	CVE-2007-2918	SendCommand_GameOver.html												
SA25514_4	CVE-2007-2918	SendTo_Exploit.html												
SA25514_4	CVE-2007-2918	SendVideo_Exploit.html												

SAID	CVE	Filename	McAfee	Norton	OneCare	ZoneAlarm	AVG	CA	F-Secure	TrendMicro	BitDefender	Panda	Kaspersky	Norman
SA25514_5	CVE-2007-2918	VAddContact_GameOver.html												
SA25514_5	CVE-2007-2918	VApplySettings_GameOver.html												
SA25514_5	CVE-2007-2918	VDeleteContact_GameOver.html												
SA25514_5	CVE-2007-2918	VDropPictures_GameOver.html												
SA25514_5	CVE-2007-2918	VGetContactUserName_GameOver.html												
SA25514_5	CVE-2007-2918	VGetPiconURL_GameOver.html												
SA25514_5	CVE-2007-2918	VImportContacts_GameOver.html												
SA25514_5	CVE-2007-2918	VImportPictures_GameOver.html												
SA25514_5	CVE-2007-2918	VInitCall_GameOver.html												
SA25514_5	CVE-2007-2918	VIsContactMember_GameOver.html												
SA25514_5	CVE-2007-2918	VIsContactOnline_GameOver.html												
SA25514_5	CVE-2007-2918	VSelectAudioInputSource_GameOver.html												
SA25514_5	CVE-2007-2918	VSelectAudioOutputSource_GameOver.html												
SA25514_5	CVE-2007-2918	VSelectVideoSource_GameOver.html												
SA25514_5	CVE-2007-2918	VSendMessage_GameOver.html												
SA25514_5	CVE-2007-2918	VSetCurrentPictureFolder_GameOver.html												
SA25514_5	CVE-2007-2918	VSharePicture_GameOver.html												
SA25514_5	CVE-2007-2918	VVibeDoctor_GameOver.html												
SA25514_5	CVE-2007-2918	VVideoMailWizard_GameOver.html												
SA25547#1	CVE-2007-3147	Exploit.html		Found!										
SA25547#1	CVE-2007-3147	GameOver.html		Found!										
SA25547#2	CVE-2007-3148	Exploit.html		Found!										
SA25547#2	CVE-2007-3148	GameOver.html		Found!										
SA25627#5	CVE-2007-2222	FileName_PoC.html		Found!										
SA25627#5	CVE-2007-2222	Find_Exploit.html		Found!										
SA25627#5	CVE-2007-2222	Find_GameOver.html		Found!										
SA25627#5	CVE-2007-2222	InitAudioSourceDirect_Exploit.html		Found!										
SA25627#5	CVE-2007-2222	DestroyResultsObject_GameOver.html		Found!										
SA25627#5	CVE-2007-2222	GrammarFromStream_GameOver.html		Found!										
SA25718#1	CVE-2007-3829	GameOver.html												
SA25718#2	CVE-2007-3829	PoC.html												
SA26011	CVE-2007-4034	GameOver.html												
SA26426	CVE-2007-4336	GameOver.html					Found!							
SA26447	CVE-2007-2223	PoC.html		Found!										
SA26579	CVE-2007-4515	GameOver_fvCom1.html		Found!										
SA26579	CVE-2007-4515	GameOver_fvCom2.html												
SA26579	CVE-2007-4515	GameOver_info.html												
SA26644	CVE-2007-4467	GameOver.html												
SA26970	CVE-2007-5217	Exploit1.html												
SA26970	CVE-2007-5217	Exploit2.html												
SA26970	CVE-2007-5217	GameOver1.html												
SA26970	CVE-2007-5217	GameOver2.html												
SA27248	CVE-2007-5601	GameOver.html												
SA27795	CVE-2007-6144	Exploit.html												
SA27795	CVE-2007-6144	GameOver.html												
SA27885#1	CVE-2007-6016	DOWText_Exploit.html		Found!										
SA27885#1	CVE-2007-6016	DOWText_GameOver.html		Found!										
SA27885#1	CVE-2007-6016	MonthText_PoC.html		Found!										
SA27934	CVE-2007-5989	PoC.html												
SA27994	CVE-2008-0935	Exploit.html												
SA28036#1	CVE-2007-3902	PoC.html												
SA28036#4	CVE-2007-5347	PoC.html												
SA28134	CVE-2007-6493	Exploit.html												
SA28134	CVE-2007-6493	PoC.html												
SA28145	CVE-2007-6530	GameOver.html												
SA28184#1	CVE-2007-4474	Exploit1.html												
SA28184#1	CVE-2007-4474	Exploit2.html												
SA28184#1	CVE-2007-4474	GameOver1.html												
SA28184#1	CVE-2007-4474	GameOver2.html												
SA28399	CVE-2007-6250	Exploit.html		Found!										
SA28399	CVE-2007-6250	GameOver.html		Found!										
SA28660	CVE-NOMATCH	GameOver1.html												
SA28660	CVE-NOMATCH	GameOver2.html												
SA28715	CVE-2008-0659	GameOver.html												
SA28757#2	CVE-2008-0625	Exploit.html		Found!										
SA28757#2	CVE-2008-0625	GameOver.html		Found!										
SA28903#2	CVE-2008-0077	Exploit.html												

SAID	CVE	Filename	McAfee	Norton	OneCare	ZoneAlarm	AVG	CA	F-Secure	TrendMicro	BitDefender	Panda	Kaspersky	Norman
SA28903#2	CVE-2008-0077	PoC1.html												
SA28903#2	CVE-2008-0077	PoC2.html												
SA28903#2	CVE-2008-0077	PoC3.html												
SA28903#3	CVE-2008-0078	PoC.html		Found!										
SA29315	CVE-2008-1309	PoC.html												
SA29328#1	CVE-2006-4695	GameOver.html												
SA29330	CVE-2007-6253	Exploit.html												
SA29330	CVE-2007-6253	GameOver1.html												
SA29330	CVE-2007-6253	GameOver2.html												
SA29408	CVE-2008-1472	Exploit.html												
SA29408	CVE-2008-1472	GameOver.html												
SA29712	CVE-NOMATCH	PoC_intOF.html												
SA29712	CVE-2008-0083	PoC.html												
SA29714	CVE-2008-1086	PoC.html		Found!										
SA29837	CVE-2008-1786	GameOver.html												
SA30037	CVE-2007-6339	PoC.html												
SA30403	CVE-2008-0955	GameOver.html	Found!	Found!										
SA30667#2	CVE-2008-2431	PoC.html		Found!										
SA30667#3	CVE-2008-2431	PoC.html		Found!										
SA30667#4	CVE-2008-2431	PoCs.html												
SA30667#6	CVE-2008-2431	PoC.html												
SA30667#8	CVE-2008-2431	Exploit.html												
SA30667#9	CVE-2008-2431	Exploits.html												
SA30709	CVE-2008-2908	GameOver1.html												
SA30709	CVE-2008-2908	GameOver2.html												
SA30709	CVE-2008-2908	GameOver3.html												
SA30883	CVE-2008-2463	Exploit.html												
SA31370	CVE-2008-2436	PoC.html												
SA31675#1	CVE-2008-2254	PoC1.html												
SA31675#1	CVE-2008-2254	PoC2.html												
SA31375#2	CVE-2008-2255	PoC.html												
SA31724	CVE-2008-3008	GameOver.html		Found!										
SA31744	CVE-2008-3007	PoC1.html		Found!										
SA31744	CVE-2008-3007	PoC2.html		Found!										

Totals (ranked by discovery rate)

SAID	CVE	Filename	Norton	BitDefender	TrendMicro	McAfee	OneCare	Kaspersky	AVG	F-Secure	Panda	ZoneAlarm	CA	Norman
All test cases			21,33%	2,33%	2,33%	2,00%	1,67%	1,00%	1,00%	1,00%	1,00%	0,67%	0,33%	0,00%
Important test cases			30,95%	3,97%	3,97%	3,97%	2,38%	2,38%	2,38%	2,38%	1,59%	1,59%	0,79%	0,00%

Source: Secunia.

Conclusion

These results clearly show that the major security vendors do not focus on vulnerabilities. Instead, they have a much more traditional approach, which leaves their customers exposed to new malware exploiting vulnerabilities.

One could argue that this isn't a problem, since no single product can offer a 100% protection. Yet, many of these suites clearly indicate that they are comprehensive and offer protection against “all” Internet threats, thus many users would rightfully expect these suites to protect them against all current threats.

The combination of security vendors not being able to detect exploits and users patching software too infrequently (almost one-third of all installed software lack one or more security related updates) leaves the door wide open for professional Internet criminals.

While we did expect a fairly poor performance in this field, we were quite surprised to learn that this area is

more or less completely ignored by most security vendors. Some of the vendors have taken other measures to try to combat this problem. One is Kaspersky who has implemented a feature very similar to the Secunia PSI, which can scan a computer for installed programs and notify the user about missing security updates. BitDefender also offers a similar system, albeit this is more limited in scope than the one offered by Kaspersky and Secunia.

We do, however, still consider it to be the responsibility of the security vendors to be able to identify threats exploiting vulnerabilities, since this is the only way the end user can learn about where, when, and how they are attacked when surfing the Internet.

This does not mean that the user shouldn't patch. On the contrary, patching remains of key importance since this is the only proper and efficient way to secure a system against covert attacks hidden in “legitimate” files and web sites.

The best of it all – patching is free-of-charge!