

By: [Aparna Chakraborty](#), Technology News Editor

[Bad, Bad Browser Plug-ins - IE, Firefox, Opera](#)

[Acrobat](#), [Flash](#), [QuickTime](#), [ActiveX](#), [Mozilla browser extensions](#), [Opera widgets](#) and [Sun Java](#)

As far as bad browser plug-ins are concerned, Symantec revealed that [Internet Explorer's](#) ActiveX is the worst. When it comes to Internet Explorer, [Opera](#) or Firefox, the browsers as standalone applications do offer end users a range of functionality and features, but at the same time their capabilities can be extended through additional solutions dubbed plug-ins or add-ons. Because of their ubiquity, browsers are one of the principal avenues for exploits looking to compromise the underlying operating systems. And in this context, plug-ins are a critical vector for attacks, as vulnerabilities in the browsers or the operating systems are increasingly difficult to exploit. In its Internet Security Threat Report Volume XIII: April, 2008, security company [Symantec](#) looked at a number of browser plug-ins and highlighted the items that are severely affected by vulnerabilities. "Browser plug-ins are technologies that run inside the Web browser and extend its features. They can include plug-ins that allow additional multimedia content from Web pages to be rendered in the browser. They can also include execution environments that allow applications to be run inside the browser. Many browsers include various plug-ins in their default installation and provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of Web browsers. Some plug-ins may even be required to use public Web sites and/or an organization's internal sites. Browser plug-in vulnerabilities are implicated in some client-side attacks and present similar challenges to the enterprise," Symantec stated. Symantec analyzed some of the most prominent plug-ins available, some of them just as ubiquitous as the browsers they are designed to enhance, if not even more so. Security flaws in Adobe Acrobat, Adobe Flash, Apple QuickTime, Microsoft ActiveX, Microsoft Windows Media Player, Mozilla browser extensions, Opera widgets and Sun Java were counted for 2007. What Symantec found is consistent with Windows and Explorer being the most attacked platform, and respectively browser available. "Vulnerabilities affecting plug-ins for Web browsers have stayed at a high watermark. We documented 239 plug-in vulnerabilities in the second half of 2007, and 237 plug-in vulnerabilities in the first half of 2007. ActiveX is still the main culprit, but we observed a drop from 210 ActiveX vulnerabilities in the first half of 2007 to 190 ActiveX vulnerabilities in the second half," explained David McKinney, Analyst, Symantec Security Response. Between July and December 2006, the Apple QuickTime plug-in was impacted by 19 vulnerabilities, with 13 plaguing Sun Java and 11 Adobe Flash. Windows Media Player had just four vulnerabilities in the second half of the past year, while Adobe Acrobat and [Mozilla browser](#) extensions had one each. "ActiveX is also an attractive target because many users may not be aware that they have installed vulnerable controls, and because of the relative difficulty of removing or patching ActiveX controls once they have been installed. The largest proportion of plug-in vulnerabilities affects ActiveX, which indicates that Internet Explorer is still the primary attack vector for plug-in vulnerabilities. However, the vast majority of these vulnerabilities affect third-party ActiveX controls. The release of [Internet Explorer 7](#) included security enhancements to limit the exploitation of ActiveX vulnerabilities; however, this has not appeared to have reduced the prevalence of ActiveX vulnerabilities. This may be a measure of the effectiveness of these security enhancements or it may indicate that many at-risks users have not upgraded to Internet Explorer 7," Symantec added.