

Re: Antivirus

Source: <http://linux.derkeiler.com/Newsgroups/alt.os.linux.suse/2004-08/2472.html>

From: srm (*user_at_example.net*)

Date: 08/13/04

Date: Fri, 13 Aug 2004 09:27:06 +0200

Paul J Gans wrote:

>> *The Symantec site lists 14 Linux viruses. But none since 2002 and most
>> were 'proof of concept' types where the payload or potential damage was
>> classed as negligible or trivial. Most required very specific
>> environments in which to operate.*
>
>
> *There are vulnerabilities in many programs that run on Linux.*

Indeed. Witness this recent report from Netcraft...

--

Recent phishing-related security problems for Internet Explorer have prompted more than a few Windows users to sample alternative browsers, including Firefox, the new open source browser from the Mozilla Project, as well as Opera.

But it turns out Internet Explorer isn't the only browser vulnerable to spoofing. On July 30 a published exploit demonstrated how to convincingly spoof a secure web site (in this case PayPal) in Firefox and Mozilla by using XML to alter the browser interface (Note: The spoof doesn't work in IE).

"The problem is that Mozilla and Mozilla Firefox don't restrict websites from including arbitrary, remote XUL (XML User Interface Language) files," Secunia writes in its analysis. "This can be exploited to 'hijack' most of the user interface (including tool bars, SSL certificate dialogs, address bar and more), thereby controlling almost anything the user sees." Notes from the Bugzilla web site indicate that the Mozilla development team was aware of the XUL problem as early as Dec. 1999 but kept the security hole confidential, apparently until the exploit was published.

On July 26, a separate Firefox spoofing issue was found, which allows a malicious website to use another site's SSL certificate to present a secure spoofed page with a "locked" icon. The exploit manipulates the cache, a directory where the browser stores web pages it has viewed. Both spoofing issues are known to affect Firefox 0.9.2, but reportedly have been fixed in the latest version, 0.9.3 (although some users say the spoofing flaw persists). The browser's official 1.0 release is tentatively scheduled for Sept. 14.

A spoofing flaw has also been found in Opera, which allowed an iframe tag to display spoofed content. The problem has been fixed in Opera 7.5.4, which was released August 5.

--