

New IE Exploit Spoofs Web Sites

By Matthew Broersma, eWEEK

December 17, 2004

Security researchers have uncovered a spoofing flaw in Internet Explorer that could allow a scammer to display a fake Web site with all of the attributes of a genuine, secure site.

Security researchers have uncovered a spoofing flaw in Internet Explorer that could turn out to be the perfect holiday gift for scammers.

The bug, which has been confirmed on a fully patched Windows XP system with IE 6.0 and Service Pack 2, could allow a scammer to display a fake Web site with all the attributes of a genuine, secure site, including the URL and the icon indicating SSL security, according to researchers.

Because the vulnerability is found in one of Internet Explorer's default ActiveX controls, scammers could use it to spoof the content of any site, researchers said. Users could be lured to the fake site via a link in an e-mail message, a tactic that continues to prove effective despite efforts to educate users. "Ordinarily, to spoof a site you have to have some issue on the Web site that you want to manipulate, which restricts what you can do," said Thomas Kristensen, chief technology officer at independent security firm Secunia, in a telephone interview. "Because this is embedded in IE by default, it's possible to inject content into any Web site. There's no way for a Web site to protect itself against this."

There is currently no patch for the bug. Users can protect themselves by turning off ActiveX or switching the security level for the "Internet" zone to "high," researchers said.

The vulnerability is caused by an error in the way the DHTML Edit ActiveX control handles certain inputs. The result is that a malicious site can execute script code in a user's browser session in the context of any other site, according to Secunia.

[Microsoft has issued a "critical" update to fix a flaw in SP2's Windows Firewall. Click here for the full story.](#)

Secunia has issued an [advisory](#) describing the issue and is offering an [online demonstration](#) to test browser vulnerability. The test displays a page with the URL "https://www.paypal.com/" and a padlock indicating a site with SSL security, but the content is supplied by Secunia.

The bug was discovered by a researcher from [Greyhats Security Group](#). Secunia's demonstration is based on a proof of concept from Greyhats.

"Once it is displaying the site, if you follow best practices and look for the padlock, et cetera, you still won't have a clue [that the site is spoofed]," Kristensen said. "It isn't really even spoofing—you are really visiting the site, it's just that another site is controlling what you see."

He said that SP2 targets more traditional vulnerabilities, such as buffer overflows, but it isn't as effective against flaws such as spoofing that can be used by scammers. Under a system with SP1 but without SP2, the flaw could be additionally used to disclose the content of local files, Secunia said.

A spokeswoman for Microsoft confirmed that the company is investigating the flaw warning. "At this time, we have not been made aware of any attacks attempting to use the reported vulnerabilities or of customer impact," she said.

"Microsoft will take the appropriate action to protect our customers, which may include providing a fix through our monthly release process or an out-of-cycle security update, depending on customer needs," the spokeswoman added.

Because the vulnerability alert was released ahead of a Microsoft patch, the company said it is "concerned" that the warning was not disclosed responsibly.

"We continue to encourage responsible disclosure of vulnerabilities," the spokeswoman said. "We believe the commonly accepted practice of reporting vulnerabilities directly to a vendor serves everyone's best interests."