Pop-up vulnerability found in major browsers

By *srlinuxx*
Created *22/06/2005 - 3:55pm*
Submitted by srlinuxx on Wednesday 22nd of June 2005 03:55:12 PM Filed under Security [1]

Several popular Web browsers contain a vulnerability that could be used by cybercriminals to steal personal data, security company Secunia has warned.

The flaw would allow a phishing attack in which a malicious JavaScript pop-up window appeared in front of a trusted Web site, Secunia said in an alert published Tuesday. This could trick a surfer into revealing data such as a password.

"The problem is that JavaScript dialog boxes do not display or include their origin, which allows a new window to open--for example, a prompt dialog box--which appears to be from a trusted site," said Secunia's advisory.

According to Secunia, the latest versions of Internet Explorer, Internet Explorer for Mac, Safari, iCab, Mozilla, Mozilla Firefox and Camino are all vulnerable. Opera 7 and 8 are affected, but not 8.01, according to Opera.

To take advantage of the flaw, a cybercriminal would have to direct a Web user from a malicious site to a genuine, trusted site such as an online bank, in a new browser window. The malicious site would then open a JavaScript dialog box in front of the trusted Web site, and a user might then be fooled into sending personal information back to the malicious site.

Microsoft has said it is investigating Secunia's claims. It encouraged surfers not to trust pop-up windows that don't include an address bar or a lock icon that verifies that it came from a certified source.

Mozilla Firefox developers have already been making moves to combat this kind of phishing attack. Back in April, a patch was developed that allows people to block Java and Flash-based pop-ups unless they came from trusted sites. Mozilla wasn't immediately available to comment on Secunia's claims.

Opera confirmed Wednesday that its latest browser, 8.01, would display the pop-up's origin, letting a user inspect its URL to see if it came from a trusted site.

"Once these things are discovered, there's a rush as everyone tries to fix the problem," Christen Krogh, Opera's vice president of engineering, told ZDNet UK.

Krogh also pointed out that Secunia had rated the vulnerability as "less critical."

"This could fool some users into giving out some data to a site that wouldn't otherwise be able to get that information. But it doesn't seem like the most important issue," Krogh said.

By Graeme Wearden
ZDNet UK [2]

Security

Source URL: http://www.tuxmachines.org/node/1450

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://news.zdnet.com/2100-1009_22-5757372.html