Hackers Can Now Read Data on Supposedly Secure Web Pages

August 26, 2016 - Earlier this month at the Black Hat Security Conference in Las Vegas, programmers revealed an exploit that allows hackers to steal information from encrypted web pages. These are pages that have an https:// in front of the domain name. They are the pages that you use to sign on to bank and brokerage accounts, fill out tax forms and pretty much any page requires a user name and password. It means that just about any private information that you share over the internet is now vulnerable and there is no fix for the problem on the horizon.

The exploit is too technical in nature to discuss how it works here. If you want to read about it, you can do so here. But for someone with some programming knowledge, using it isn't all that complicated. The only thing that is required is that victims encounter a malicious JavaScript file while on the Internet. That file can be embedded in a page, served by an advertisement, etcâ€¦ It doesn't have to be on the page that the hackers are attempting to get information from.

Once a victim encounters the JavaScript file, hackers can target users visiting a particular pageâ€¦ say, a particular bank. From there they can potentially steal the victim's user name and password and then drain their account. Depending upon the site and the information stored there, they may also be able to discover your birth date, SSN, home address and even credit card numbers that you have setup to pay out of your bank accounts.

The only known way to stop the exploit is to disable acceptance of "third party cookies" in your browser. Unfortunately, some internet sites won't work if you disable these. A work around - and we have not verified this - might be to install two browsers on your computer or phone. In one, disable third party cookies and only use that browser to sign on to financial accounts. Use the other one for everyday browsing.

According to a source in the linked article above, the exploit has never been used and it has been around for the past three years. It has apparently been a known issue to HTML and browser developers for that period of time but it hasn't been fixed because doing so isn't "trivial". Now that the exploit has been reveal to everyone, it is highly likely to be used by hackers.

As always, ACCESS is advising that our readers use safe browsing habits. Only visit known websites. Don't click on links in email that you aren't expecting. Make sure your antivirus and antimalware software is installed and is up to date. These things will at the very least help protect you.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here.

Registration is easy and free.
Follow me on Twitter:

Follow ACCESS