

Re: Microsoft IE cookies readable via about: URLs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-11/0058.html>

From: Clover Andrew (aclover@lvalue.com)

Date: 11/12/01

Subject: Re: Microsoft IE cookies readable via about: URLs
Date: Mon, 12 Nov 2001 16:14:43 +0100
Message-ID: <D58B0195B58937489E89124469E57CA249DA09@EX1.lvalue.com>
From: "Clover Andrew" <aclover@lvalue.com>
To: <bugtraq@securityfocus.com>

Nick FitzGerald <nick@virus-l.demon.co.uk> wrote:

> *This was hinted at in Andrew Clover's message of 19 October*

Yes. I noted that "IE incorrectly applies HTTP-style URL parsing to 'about:' URLs", from which I really should have investigated further to find that in fact it doesn't recognise the difference between http: and about: at all in the case of cookie access security. My bad – having found what I considered enough of a hole to require patching, I didn't go further and find its full potential.

> *That's interesting, given they seemed to think there was no
> problem (despite the flaw being obvious to the rest of the
> world) back when Andrew mentioned it...*

Well, my exploit was less serious than this, but it was indicative of brokenness, and I would have expected the IE team to at least investigate. Instead, Microsoft seemed more interested in arguing Mitigating Factors. It would be easiest to simply remove the about-unknown-page-echoing-"feature", since it is of no legitimate use whatsoever (or at least enforce HTML-escaping on it). I do not expect the patch for Jouko's more serious exploit to do so, when it's released, but there's always hope.

> *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
> Settings\ZoneMap\ProtocolDefaults\about = 4*

Indeed, I've been using this a while with no problems, recommend it.

--

Andrew Clover
Technical Consultant
lVALUE.com AG

SecurityFocus Bugtraq: Re: Microsoft IE cookies readable via ab

- **Previous message:** Jeffrey W. Dronenburg: "Re: Microsoft IE cookies readable via about: URLS"
- **Maybe in reply to:** Jouko Pynnonen: "Microsoft IE cookies readable via about: URLS"
- **Next in thread:** Kristian Strickland: "Re: Microsoft IE cookies readable via about: URLS"
- **Next in thread:** Oliver Petruzel: "RE: Microsoft IE cookies readable via about: URLS"
- **Next in thread:** Thomas Reinke: "Re: Microsoft IE cookies readable via about: URLS"
- **Reply:** Kristian Strickland: "Re: Microsoft IE cookies readable via about: URLS"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]