

RE: [Full-Disclosure] Re: Re: GAYER THAN AIDS ADVISORY #01: IE 5 remote code execution

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-02/1124.html>

From: Paul Schmehl (pauls_at_utdallas.edu)

Date: 02/19/04

To: full-disclosure@lists.netsys.com

Date: Wed, 18 Feb 2004 22:29:51 -0600

—On Wednesday, February 18, 2004 9:50 PM -0500 Bill Royds
<full-disclosure@royds.net> wrote:

- > *Last time I was at my doctor's medical clinic, I noticed all the shiny new*
- > *LCD monitors showing the Windows logon prompt with account Administrator.*
- > *I asked the receptionist why. She said so that anyone could sign on any*
- > *machine when they needed it, since individual machines lock out so only*
- > *signed user or administrator can sign on. They did have the screensaver*
- > *timeout so people off the street couldn't sign on. But the only way to*
- > *make the multiple workstations usable from for anybody was to use*
- > *administrator account on all of them.*
- > *This is a bit of a design flaw in the Windows network that means*
- > *security is much less than it ought to be.*
- >

This is no more of a design flaw than it is in Unix. Replace all those Windows boxes with Unix (if you could find the software they need to use), and those people will be logging in as root on all those machines.

The problem in this case is a lack of understanding on the part of the people implementing the solution, **not** a design flaw in the software. They could just as easily create network accounts that would allow each of them to login as users on every machine in the office, if needed. Then **logout** when they're done instead of locking the machine. Or use Fast User Switching and local accounts, and anyone could login no matter who was logged in before.

Of course they would have to learn how to create a Windows domain using either a Windows server or unix with samba or learn how to use Fast User Switching (or in the case of unix, NFS or LDAP or some other mechanism to allow logins on multiple machines), but the fact remains that this is an **implementation** problem, **not** a software design flaw.

If I lock my RedHat box during an X session instead of logging out, guess who can login? Me or root.

Full-Disclosure: RE: [Full-Disclosure] Re: Re: GAYER THAN AIDS ADVISORY #01: IE 5 remote code execution

Paul Schmehl (pauls@utdallas.edu)
Adjunct Information Security Officer
The University of Texas at Dallas
AVIEN Founding Member
<http://www.utdallas.edu>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>