

Re[2]: SECURITY.NNOV: file locking and security (group policy DoS on Windows 2000 domain)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2001-12/0099.html>

From: 3APA3A (3APA3A@SECURITY.NNOV.RU)

Date: 12/08/01

Date: Sat, 8 Dec 2001 12:21:45 +0300
From: 3APA3A <3APA3A@SECURITY.NNOV.RU>
To: Seth Arnold <sarnold@wirex.com>

Hello Seth,

I never intended to review all possible locking mechanism. In advisory I ment BSD-compliant flock()/fcntl()/open() file locking implemented in most unix-like systems.

X/Open lockf() mechanism ported to few operation systems requires file to be open for writing, so, it's behind advisory (I'm talking about READ access).

P.S. I don't use linux.

—Saturday, December 08, 2001, 4:15:48 AM, you wrote to bugtraq@securityfocus.com:

SA> On Fri, Dec 07, 2001 at 11:57:58AM +0300, 3APA3A wrote:
>> *The way file locks interfere with file access depends on OS. There are 2*
>> *possible situations: moderate and non-moderate file locks. *BSD and*
>> *linux use non-moderate locking, while Windows NT locking is moderate.*
>> *What does it mean? Under Unix file locking is only checked then another*
>> *application tries to lock the file. If application doesn't use file*
>> *locking it will not be affected by file locking.*

SA> 3APA3A -- close....

SA> A long-time feature of many Unix systems, including Linux (and probably
SA> all the BSDs too, but I don't know this for sure) is mandatory file
SA> locking, implemented in the kernel. It can be turned on using the setgid
SA> bit on regular files.

SA> Look for Documentation/mandatory.txt in the linux kernel source tree. It
SA> has all the gory details on mandary file locking, as it is implemented
SA> in the linux kernel. (Or, was implemented, in 1996.. :)

SA> Cheers!

--

~/ZARAZA

Ñýð Èñääé Íüþðíí íðéðúë, +ðí ýáëíêè ìääàþð íà çâìëþ. (ðääí)

- **Previous message:** [signal 9: "Netscape engineers are weenies?"](#)
- **In reply to:** [Seth Arnold: "Re: SECURITY.NNOV: file locking and security \(group policy DoS on Windows 2000 domain\)"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)