It rather involved being on the other side of this airtight hatchway: Consequences of enabling the kernel debugger

devblogs.microsoft.com/oldnewthing/20100511-00

May 11, 2010

Raymond Chen

In the category of dubious security vulnerability, I submit for consideration the following report:

> A machine with the kernel debugger enabled is vulnerable to a denial of service attack from an unprivileged user. The unprivileged user need only deference a null pointer. Once this occurs, the computer becomes completely unusable to all users.

Um, yeah. That's sort of the whole point of the kernel debugger, to halt system execution as soon as a problem has been detected. Enabling the kernel debugger requires administrative privileges, so it's not like unprivileged users can force a system halt on their own; they need the help of an administrator to turn on kernel debugging first. At that point, you've already made it to the other side of the airtight hatchway. If you have an accomplice who is already an administrator, then you may as well just cut to the chase and tell your accomplice to add you to the administrators group, too. Then you can do much more than simply halting the system.

Clarification: As Bob noted, and which I apparently didn't make clear enough from the title of the article, this message arrived as a security vulnerability report. It's not a security vulnerability if it requires assistance from an administrator to pull off.

Raymond Chen

Follow