

Re: help

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-09/24537.html>

From: Rock (*rock_at_comcast.nospam.net*)

Date: 09/20/04

Date: Sun, 19 Sep 2004 18:47:38 -0700

Helen Minor wrote:

- > *Has anyone received a message like this before? I am*
- > *being asked to send \$19.95 to receive this patch? Please*
- > *advise Microsoft Security Bulletin MS03-043*
- > *Buffer Overrun in Messenger Service Could Allow Code*
- > *Execution (828035)*
- > *Issued: July 22, 2004*
- > *Version Number: 1.1*
- >
- > *Summary*
- > *Who Should Read This Document: Customers using Microsoft®*
- > *Windows®*
- >
- > *Impact of Vulnerability: Remote Code Execution*
- >
- > *Maximum Severity Rating: Critical*
- >
- > *Recommendation: Microsoft® Windows® should install a*
- > *patch immediately*
- >
- > *Caveats: None*
- >
- > *Tested Software and Patch Download Locations:*
- >
- > *Affected Software:*
- >
- > *Microsoft Windows NT Workstation – Download a fix to*
- > *patch this issue*
- > *Microsoft Windows NT – Download a fix to patch this issue*
- > *Microsoft Windows 2000 – Download a fix to patch this*
- > *issue*
- > *Microsoft Windows XP – Download a fix to patch this*
- > *issue*
- > *Microsoft Windows Win98 – Download a fix to patch this*
- > *issue*
- > *Microsoft Windows Server 2003 – Download a fix to patch*

- > *this issue*
- > *Non Affected Software:*
- >
- > *Microsoft Windows Millennium Edition*
- > *The software listed above has been tested to determine if*
- > *the versions are affected. Other versions are no longer*
- > *supported, and may or may not be affected.*
- >
- > *Technical Description:*
- >
- > *A security vulnerability exists in the Microsoft®*
- > *Messenger Service that could allow arbitrary code*
- > *execution on an affected system. The vulnerability*
- > *results because the Messenger Service does not properly*
- > *validate the length of a message before passing it to the*
- > *allocated buffer.*
- >
- > *An attacker who successfully exploited this vulnerability*
- > *could be able to run code with Local System privileges on*
- > *an affected system, or could cause the Messenger Service*
- > *to fail. The attacker could then take any action on the*
- > *system, including installing programs, viewing, changing*
- > *or deleting data, or creating new accounts with full*
- > *privileges.*
- >
- > *Mitigating factors:*
- >
- > *Messages are delivered to the Messenger service via*
- > *NetBIOS or RPC. If users have blocked the NetBIOS ports*
- > *(ports 137–139) – and UDP broadcast packets using a*
- > *firewall, others will not be able to send messages to*
- > *them on those ports. Most firewalls, including Internet*
- > *Connection Firewall in Windows XP, block NetBIOS by*
- > *default.*
- > *Disabling the Messenger Service will prevent the*
- > *possibility of attack.*
- > *On Windows Server 2003 systems, the Messenger Service is*
- > *disabled by default.*
- > *Severity Rating:*
- >
- >
- >
- > *Windows NT Critical*
- > *Windows Server NT 4.0 Terminal Server Edition Critical*
- > *Windows 2000 Critical*
- > *Windows XP Critical*
- > *Windows Server 2003 Moderate*
- >
- >
- >
- > *The above assessment is based on the types of systems*

microsoft.public.windowsxp.general: Re: help

- > *affected by the vulnerability, their typical deployment*
- > *patterns, and the effect that exploiting the*
- > *vulnerability would have on them.*

It's a scam. MS updates are free.