

ICS G2 Security Update

Spacelabs Healthcare response to Win32/Conficker worm

Overview

The Win32/conficker worm has been in circulation for a number of months. It is an exceptionally sophisticated worm that exploits vulnerability in the "server" service found in all versions of Microsoft Windows from Windows 2000 forward. When it infects a system it installs itself in such a way that it is nearly undetectable and falsely reports that the system is patched with the MS08-067 patch intended to protect against it. Recent reports indicate that the Win32/Conficker (variant D) worm may surface again on April 1st, 2009.

To protect ourselves and our customers, Spacelabs Healthcare systematically applies patches to all computer systems, both in our product verification and validation labs as well as our internal network infrastructure.

Product Status

As part of our standard operating procedures Spacelabs verification and validation test lab systems are patched for all Microsoft "High Priority Updates" whenever a new product enters the Verification and Validation test labs. The most recent version (4.01.02) of our ICS G2 product suite was recently released and was validated with the MS08-067 patch in place for Windows XP, Windows Vista and Windows Server 2003.

Earlier versions of ICS have not been specifically tested with this patch in place. FDA guidance in this situation recommends: "If not patching a system poses more risk than patching it, the system should be patched." Given that less than 1% of the code base changed in ICS G2 and no issues were discovered during G2 validation testing, it is reasonable to expect that applying this patch to older ICS system would be less risky than not patching. Customers are therefore advised to patch these systems prior to April 1st.

Detailed description of Win32/Conficker:

<http://www.microsoft.com/security/portal/Entry.aspx?name=Win32/Conficker>

Best defense - Link to MS08-067

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

Recovery Procedure:

<http://support.microsoft.com/kb/962007>