

Intellex[®] Security Bulletin:
FAQ Regarding Intellex and the Blaster Worm
TB_20030825_r030912
2003-Aug-25 (Revised: 2003-Sept-12)

Background

Intellex is an embedded application that runs on a Microsoft[®] Windows[®] operating system which has been specially configured to improve performance and to reduce vulnerability to malicious attack. Because of its special configuration, Intellex is not vulnerable to most common strains of computer viruses and worms propagated through email and Internet access. In fact, until recently, there has not been a documented case of a factory configured Intellex being infected by a computer virus.

The recent *Blaster*, *LovSan*, and *Welchia* worms, however, exploit a previously unknown vulnerability in the Windows 2000 operating system never before used as a pathway of attack. The vulnerability is found in an aspect of the operating system crucial to its functionality in a networked environment. (For additional technical details, please consult [Microsoft Security Bulletin MS03-039 \[Knowledge Base Article #824146\]](#).) Unfortunately, the operating system configuration used by Intellex software v3.x shares this vulnerability.

The vulnerability exploited by these new worms is easily corrected by installing the *Intellex v3.x Security Update* now available from our website, www.americandynamics.net. (Note: *Intellex v3.x Security Update* is the same as Microsoft's *Security Update for Windows 2000 – Windows2000-KB824146-x86-ENU.exe*.)

And, if your Intellex v3.x system has become infected, tools exist for easily removing the virus; we have supplied a link to these tools for you from the update download page. (See "How can I fix this vulnerability?" below for more information.)

If you have any questions not answered by the FAQ regarding Intellex, please feel free to contact American Dynamics Technical Services, via email at adtechservices@tycoint.com or via telephone at 800-507-6268, Option 2 (US) or 561-912-6259, Option 2 (International).

What Intellex systems are vulnerable?

Every DV8000, DV16000, and RMS system that has Intellex software versions 3.0 or 3.1 potentially has the Microsoft operating system security flaw unless this patch has been installed.

To determine what version of software you are running, click on *Utility, About Intellex*. If the version displayed is 3.0.xx or 3.1.xx then the security flaw must be patched.

To determine if the patch is already installed (either at the factory, or during a support maintenance visit), see "*How do I know if the patch was installed?*" below.

Systems with Intellex software versions 2.x use the Windows 98 operating system and do not have this security flaw. This includes all current versions of Intellex LT as well as Intellex v2.0 to v2.5 software.

How can I fix this vulnerability?

The corrective actions to prevent attack by these worms and to remove the worm software are described on the American Dynamics web site, www.americandynamics.net, under the *Software Downloads* page.

The steps required are:

1. Install the *Intellex v3.x Security Update*, to correct the vulnerability. (Note: *Intellex v3.x Security Update* is the same as Microsoft's *Security Update for Windows 2000 – Windows2000-KB824146-x86-ENU.exe*.)
2. Run a scan program, *Stinger.exe*, developed by Network Associates Incorporated, to detect and remove the virus if your computer is already infected.

Both the security patch and the scanning software are available via the American Dynamics web site, www.americandynamics.net, in the *Software Downloads* section of the site.

How do I know if the patch is installed?

Since the security patch applies to the operating system and was not developed by American Dynamics, it is not possible to determine if it is installed from the Intellex menus. You must exit the Intellex application and check the operating system updates by performing these steps:

1. Exit the Intellex application by clicking on *Utility, Exit*.
2. Click on *Yes* and enter the eight-digit PIN number when prompted. (Note: contact your System Administrator to obtain the PIN number.)
3. Double click on *My Computer*.
4. Double click on *Control Panel*.
5. Double click on *Add/Remove Programs*.
6. Using the scroll bar on the right side of the window, look for a program called "Windows 2000 Hotfix-KB824146". If this program is present the security patch is already installed.
7. If the program is not present, then the security patch is NOT installed and you must perform the corrective action described above.

Network administrators can use a scanning tool available from Microsoft to check each Intellex on a network. (For additional technical details, please consult [Microsoft Security Bulletin MS03-039 \[Knowledge Base Article #824146\]](#).)

What if I use the Intellex Recovery CD after the patch has been installed?

If you use the recovery CDs provided with the Intellex after the patch was installed, you MUST re-install the security patch. If you do not re-install the security patch, the Intellex will be vulnerable to these viruses. Monitor the American Dynamics web site, www.americandynamics.net, for up to date information on virus protection for Intellex.

How do I prevent another virus attack?

Once the security patch is installed, any worm or virus that attacks this security flaw in the operating system cannot infect the Intellex.

In general our recommendation to prevent attacks by viruses and worms are:

- Do not use the Intellex for email, World Wide Web access, or general computing applications.
- Do not install any software that is not approved for use by American Dynamics.
- Do not change the operating system configuration.
- Do not enable the Server or Messenger services in the operating system.
- Do not share the hard drives on the Intellex across a network.
- Always verify that any media used to update the Intellex software is free from viruses. When downloading software from the American Dynamics web site and copying to removable media for transfer to the Intellex, always use a PC that is free from viruses.
- Always use a firewall if the network is connected to the Internet. Open only the ports necessary for Network Client access.
- Always control physical access to the Intellex to prevent unauthorized personnel from changing the software or operating system configuration.
- Monitor the American Dynamics web site, www.americandynamics.net, for up to date information on virus protection.

Should I install anti-virus software on the Intellex?

American Dynamics strongly recommends against installing virus protection software on the Intellex. Most virus protection software continuously monitors all files that are read and written to the hard disk and this can affect the video recording function that the Intellex performs. American Dynamics is evaluating additional virus protection measures for Intellex and will be providing more information via the American Dynamics web site as soon as it is available.

CONTINUOUS IMPROVEMENT STATEMENT

As with all processes defined by the American Dynamics Technical Services Group, this document is intended to be a work in progress. Further refinements and suggestions are welcome and should be sent in writing to the owner/author of this document as listed below.

CONTACT INFORMATION

If you have any questions regarding this bulletin, please contact American Dynamics Technical Services at:

Toll Free: 800-507-6268, Option 2
 International: 561-912-6259, Option 2
 Fax: 845-624-7658
 Email: adtechservices@tycoint.com

Information furnished by American Dynamics is believed to be accurate and reliable. However, no responsibility is assumed by American Dynamics for its use, nor any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent rights of American Dynamics.