

AMB2004-05

April 30, 2004

Virus Immunity and AMOS® 8.0 A Significant Sales Advantage - Use It!

Dear Alpha Micro VAR:

AMOS 8.0 uses Microsoft's Windows XP Embedded® (“XPE”) operating system for many supporting services, including low level networking. Previous versions of AMOS have been completely immune to network-related viruses. Many VARs have inquired as to whether AMOS 8.0 is now subject to certain virus risks as a result of using this Microsoft software.

The answer is a simple one: Keep the configuration a purely AMOS system, and AMOS 8.0 remains as immune as all other AMOS systems have been.

Specifically, AMOS 8.0 uses the same AlphaTCP as other AMOS systems. Any new network-related virus weakness depends upon the Microsoft features we install and activate. We only install and activate Microsoft features needed to support AMOS 8.0. There is no Microsoft Web Server, no Microsoft E-mail, etc.

To block network viruses on the XP Embedded side, we now fully activate the XP firewall for all Ethernet interfaces. We also install but disable Microsoft File and Printer sharing. Enabling parts of File and Printer Sharing is under the control of the system administrator - AMOS 8.0 and AlphaTCP work fine without them.

While it may be tempting to enable Microsoft File and Printer Sharing so that an AMOS 8.0 server can also function as a peer-to-peer network server, please be aware that this particular function more than any other would make the AMOS server susceptible to outside attacks. Think carefully before you take this step.

The XPE Firewall Configuration

XPE includes a basic firewall. This firewall has no effect on AMOS 8.0 network traffic but can isolate XPE from any network traffic. We now ship AMOS 8.0 systems with the XPE firewall fully enabled. (Previously, it was configured with just a few ports open to support the Microsoft File and Printer Sharing.) If you have any questions, please contact us or, if you like, we can work with your system administrator to check or change the settings.

Patches Available From Microsoft

As patches are made available from Microsoft, we incorporate them into future builds and release those that can be dynamically done in the field. However, only a very few apply to the components we install. Because the XPE features, by Microsoft's design, are "locked down" at build time for each system, the system may have to be rebuilt here at the factory to install some patches.

Alpha Micro's Own In-House Experience

We configured our in-house "am-8000.alphamicro.com" demonstration system, attached to the Internet, without any firewall for months last year. AMOS 8.0 was never damaged nor compromised! Among the many attacks, the RPC Service attacks were the only ones that affected XPE. These attacks disabled (rather than opened) some RPC services, having no effect on AMOS 8.0 and only a temporary affect on XPE.

Since re-activating XPE's Firewall on XPE's Internet interface, we have had no virus related issues. The AM-8000 has two Ethernet interfaces. We configured the second one on our private network with some firewall holes for Microsoft File and Printer Sharing. As the AlphaTCP IP address is different than the XPE's IP address, the Eagle 800 can be similarly protected with an external firewall.

If someone wants to hammer at our AM-8000's Microsoft Internet interface, it is usually 66.166.1.34. Please let us know if you see any weaknesses! We will tighten up any openings that you discover.

How To Make AMOS Virus-Proof

For systems manufactured after March 5, 2004, do nothing. For systems manufactured prior to March 5, 2004, make sure the XPE Firewall is fully enabled and neither local XPE paths nor local XPE printers are configured for Microsoft sharing.

Advantage: AMOS

Virus susceptibility is an extremely important issue in today's computer network environment. AMOS servers' virus immunity is a unique sales advantage - use it to your advantage, both from a sales and technical standpoint!

If you have any comments or questions regarding this issue, please contact our Technical Support Department at (800) 487-7877.