

# Unisys e-@ction Enterprise Servers Security Notice

The default security settings on this server may be inadequate for your environment. In addition, security vulnerabilities may have been discovered after this software was released. UNISYS MAKES NO CLAIM OR WARRANTY THAT YOUR SYSTEM IS SECURE AS DELIVERED.

Before you connect this server to a network, review the security requirements of your applications, data, and environment. On cellular multiprocessing (CMP) servers, be sure to evaluate the operating system on the Service Processor(s) as well as each partition's operating system. Then implement an appropriate security policy.

**Note:** Review your security policy and current information on security vulnerabilities on a continuing basis and update your system as appropriate.

Systems with Web services installed, such as Microsoft Internet Information Services (IIS), may require added security considerations. You should be aware that IIS components are installed on several Unisys servers by default, such as ES5000, ES7000, CS, LX, NX, and IX systems. This should be taken into account in performing your security review.

## Microsoft Operating Systems

Microsoft provides security information on their Web site at

<http://www.microsoft.com/technet/itsolutions/security/default.asp>

The latest information on security vulnerabilities is available from Microsoft at

<http://www.microsoft.com/technet/itsolutions/security/current.asp>

Unisys recommends that you register to automatically receive Microsoft Security Bulletins. On either of the Web sites listed above, click the link titled "Want to receive future security bulletins automatically?"

## Windows Datacenter Customers

Customers using Windows 2000 Datacenter must obtain patches only from Unisys, or their Datacenter certification may be affected. A patch downloaded directly from Microsoft may fail to install on a Datacenter system. Datacenter customers can request a security patch or other Microsoft hotfixes by submitting a Support Request or User Communication Form (UCF) against the product WIN-DATACENTER. Include the following in the headline:

requesting xxxx

where xxxx indicates the Microsoft article describing the fix or update you need.

In the details, include information that Unisys will need to evaluate and track your request. This includes

- Customer name and address
- Customer contact person and phone number
- System Serial Number (for example, 491519232)
- Service Processor Release level (for example, 8.1.1)

Please provide the following information for each partition on which the update will be installed:

- System or partition name
- Datacenter Service Pack level (for example, base or SP2)
- Certification level or MID number (for example, 8.1.c1 or 42000)

Once Unisys has all the necessary information, Unisys can then verify that requested patches are appropriate for your environment and whether they have been adequately tested. These UCFs will be handled promptly upon receipt.

## **ClearPath Customers**

Customers running ClearPath servers are reminded that while the main function of their server is an MCP or OS 2200 operating environment, there may be one or more Windows 2000 or Windows NT operating systems running on the platform. These environments should follow the same guidelines as other Microsoft operating system servers.

## **ClearPath NX: UnixWare OS on System Control Processors**

Customers running UnixWare on System Control Processors (SCPs) that are available on a public network, or who have other security concerns should review security advisories. You can view potential problems and the associated fixes by going to the following Web site:

<http://www.caldera.com/support>

Click on the link "Security Advisories for UNIX" for patches for your system.

Customers must obtain patches from Unisys. A directly downloaded patch may be incompatible with other SCP software. Customers can request a security patch by submitting a support request against the hardware product (for example, NX6830). Include the advisory reference number in the request.

## **UNIX Operating Systems**

Caldera has identified several potential security holes in the UnixWare and Open UNIX 8 operating systems. You can view a table of potential problems and the associated fixes by going to the following Web site:

<http://www.caldera.com/support>

Click on the link "Security Advisories for UNIX" for patches for your system.

## **Novell NetWare**

Customers using Novell NetWare servers can look for security information at the Novell support site at

<http://support.novell.com/>



78627205-000