UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

August 29, 2003

NRC INFORMATION NOTICE 2003-14: POTENTIAL VULNERABILITY OF PLANT COMPUTER NETWORK TO WORM INFECTION

Addressees

All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

Purpose

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to alert addressees to the recent identification of a potential vulnerability of the plant computer network server to infection by the Microsoft (MS) SQL Server worm. The NRC anticipates that recipients will review the information for applicability to their facilities and consider taking appropriate actions to prevent the MS SQL Server worm from infecting their plant network servers. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response is required.

Background

Microsoft (MS) SQL Server 2000 is a database software program for network servers. The program contains a remotely exploitable stack buffer overflow that is vulnerable to potential hackers. When an overflow occurs, arbitrary code can be executed on the victim system with the user privileges of the SQL Server. Once a server is compromised, the MS SQL Server 2000 Worm propagates itself by making packets of 376 bytes and sending them to randomly chosen Internet Protocol (IP) addresses User Datagram Protocol (UDP) port 1434. If the packet is sent to a vulnerable machine, the machine becomes infected and begins to propagate. This worm activity is readily identifiable on the computer network by the presence of 376-byte UDP packets. Microsoft Corporation identified this vulnerability in the SQL Server 2000 and issued a security patch on July 10, 2002. When Microsoft Corporation releases a patch to fix a problem for its software, the full details of the vulnerability of the product are disclosed.

Description of Circumstances

On January 25, 2003, Davis-Besse nuclear power plant was infected with the MS SQL Server 2000 worm. The infection caused data overload in the site network, resulting in the inability of the computers to communicate with each other. The slowness in computer processing speed began in the morning and by 4:50 p.m., the Safety Parameter Display System (SPDS) became

unavailable and remained unavailable for 4 hours 50 minutes. By 5:13 p.m., the plant process computer was lost and remained unavailable for 6 hrs and 9 minutes. Although the operators were burdened by these losses, the event was not deemed significant since the plant control and protection functions were not affected.

Because the MS SQL worm resided in only memory, shutting down the server removed the worm from the server's memory, ridding the server of the infection. The licensee isolated the server from the site network, installed the MS security patch, and reconnected the server to the site network.

Discussion

First Energy Nuclear's (the licensee's) corporate network, which is linked with Davis-Besse's plant network, is connected to external networks via a firewall. A firewall is a system or systems that enforce an access control policy between networks. Among the many access control policies that Davis-Besse's corporate firewall enforced was the policy of disallowing any data using the UDP into the network by closing port 1434 of the firewall. This policy would have protected Davis-Besse's networks from the MS SQL worm infection except that the corporate network had a T1 connection behind the firewall that provided a path for the worm to enter the system. This T1 line was used by one of the licensee's consultants who provided an application software that ran on a server. This connection bypassed all the access control policies that the corporate firewall was enforcing, including the policy of preventing data that used the UDP from coming into the corporate network.

The consultant's company network server allowed use of the UDP for data transfers and was infected by the MS SQL worm. When the consultant established a T1 line connection at the licensee's corporate site, this action opened a path by which the worm that infected the consultant's company server was sent to the licensee's corporate network through the T1 line. The worm then randomly infected any servers on the corporate network that had port 1434 open.

Two primary causes for this worm infection were noted:

1. The T1 connection behind the firewall

   The corporate network would not have been infected by the worm if the consultant's T1 line had been connected in front of the firewall. In February 2002, the NRC issued a security order which alerted licensees to external connections that bypass network protective measures. Subsequent to this event, the licensee noted that the implementation of the order was addressed by the Information Technology personnel; however, their activities were not communicated to the plant computer engineers.

2. Unawareness of Software Security Patch

   The plant computer engineering personnel had not been aware of the security patch that Microsoft released on July 10, 2002, to fix the Microsoft SQL Server 2000 vulnerability that the MS SQL worm exploited. In addition, on January 25, 2003, Microsoft issued an alert about the MS SQL worm. On the same day, CERT Coordination Center, a

federally funded research and development center that provides Internet security expertise, also issued Advisory CA-2003-04, MS-SQL Server Worm. A revision to this advisory was issued on January 27, 2003.

In response to this event, Davis-Besse implemented the following corrective actions: (1) required network services to document all external connections to internal network, (2) installed the security patch for the MS SQL Server 2000 vulnerability, (3) installed a firewall between the plant network and the corporate network, (4) established a requirement to monitor and filter the data coming into the plant network to the same standard as the corporate firewall, and (5) implemented a process for computer engineering personnel to review security patches for systems supported and install them within an acceptable timeframe.

This information notice requires no specific action or written response. If you have any questions about the information notice in this notice, please contact one of the technical contacts listed below or the appropriate project manager in the NRC's Office of Nuclear Reactor Regulation (NRR).

/RA/
William D. Beckner, Chief
Reactor Operations Branch
Division of Inspection Program Management
Office of Nuclear Reactor Regulation

Technical contacts: Samuel S. Lee
(301) 415-1061
E-mail: ssl@nrc.gov

Matthew Chiramal
(301) 415-2845
E-mail: mxc@nrc.gov

Eric J. Lee
(301) 415-8099
E-mail: exl@nrc.gov

Attachment: List of Recently Issued NRC Information Notices