NOPSA

NATIONAL OFFSHORE PETROLEUM SAFETY AUTHORITY

SAFETY ALERT 43

Malware Threat to Industrial Control Systems

What happened?

IT security researchers have identified malware that is specifically designed to search out and attack supervisory, control and data acquisition (SCADA) systems. It is believed that the main means of spreading this malicious code is via USB storage devices.

When the USB storage device is opened in Windows Explorer, or any other file manager that can display file icons, the exploit uses a previously undetected vulnerability in Windows to infect the operating system.

The exploit triggers even if the autostart function in Windows is completely disabled. No file has to be opened for the infection to take place.

What could go wrong?

The exploit could allow third parties to interfere with SCADA systems, potentially causing an increase in demand on independent safety related systems through maloperation of a process.

Key Lessons:

While this malware appears to be aimed specifically at Siemens systems, it establishes the principle that it is possible to create malicious code specifically aimed at SCADA systems, and serves as a timely reminder to Operators to ensure that effective measures are in place to guard against malware infection.

As the malware uses root kit techniques, there is the possibility that it cannot be detected on a running system. Users of Siemens' WinCC or Step7 software should therefore scan their systems with current antivirus-software using a rescue CD. For details you should contact your local antivirus support.

Contact

For further information email alerts@nopsa.gov.au and quote Alert 43.