ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-10-239-01: DYNAMIC LIBRARY LOADING VULNERABILITY IN MICROSOFT-BASED APPLICATIONS

August 27, 2010

ALERT

SUMMARY

ICS-CERT is aware of reports describing a method to load attacker-supplied DLLs in vulnerable Microsoft Windows applications. A number of potential mitigations, including the ability to limit the application DLL search path, have been provided in Microsoft Security Advisory 2269637. Additional details and references have been provided in US-CERT Technical Alert TA10-238A and VU Note #707943.

Of note to industrial control systems environments is the fact that DLL safe search mode is disabled by default in Windows 2000 Service Pack 4 and Windows XP prior to Service Pack 3. Windows 2000 versions prior to Service Pack 4 do not support DLL safe search mode. While this feature does not prevent the exact same types of attacks, it does provide mitigation on a local system by forcing a specific order of DLL loading. Without DLL safe search mode enabled, the current directory is searched before any system level directories. This provides an attacker with the opportunity to drop a malicious DLL with the same name as a system DLL in the current directory and have it be executed prior to the valid DLL file. Microsoft has published an article outlining details about DLL search order on Microsoft Windows systems.

Environments which have implemented defense in depth measures like outbound firewall filtering and limiting or eliminating web and E-mail access are well postured to defend against these risks. Owner/operators with those mitigations in place should continue to focus on alternate weak points like the introduction of malicious code through USB drives as seen with Stuxnet.

ICS-CERT recommends industrial control systems vendors review their software to determine if any of their applications are vulnerable. Microsoft has published an article describing how to properly implement DLL security in Windows-based applications.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT Operations Center
1-877-776-7585
www.ics-cert.org
ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.