ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-10-211-01: MICROSOFT ANNOUNCES OUT-OF-BAND UPDATE

July 30, 2010

ALERT

ICS-CERT Advisory ICSA-10-201-01 provided information on newly discovered malware which targets Siemens industrial control systems. The malware utilizes a Microsoft Windows vulnerability that exists due to Windows' failure to properly obtain icons for .LNK files.

Microsoft has scheduled the release of an out-of-band security bulletin for Monday, August 2, 2010. According to Microsoft, the bulletin will address this security vulnerability in all supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

ICS-CERT recommends control system owners/operators review the Microsoft Notification and the US-CERT Critical Infrastructure Information Notice CIIN-10-204-01A UPDATE-July 30, 2010.

This CIIN is located on the US-CERT Portal in the following library location:

"ICS-CERT/US-CERT Critical Infrastructure Information Notices (CIINs)/ CIIN-10-204-01A-Microsoft .LNK Vulnerability "

The Microsoft Security Bulletin Advance Notification for August 2010 can be found at the following URL:

http://www.microsoft.com/technet/security/bulletin/ms10-aug.mspx

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.