NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Recommendation to Industry

CIP: Microsoft Out-of-Band Security Bulletin MS08-067
October 24, 2008

Status:	**Acknowledgment of Receipt Required By October 28, 2008.**
Responsible Entities:	All Registered Entities
Primary Interest Groups:	Generation, Transmission, Control Centers, SCADA, EMS; Users of Microsoft Windows Platforms
Recommended Action:	All recipients of this Recommendation should review the materials provided by Microsoft and determine appropriate mitigating steps to address this vulnerability. Recipients should note that not all mitigations and workarounds (specifically blocking ports or disabling services) from the MS08-067 bulletin are appropriate for control systems. All recipients of this Recommendation should contact their control system (EMS, SCADA, Substation Automation, Plant Control, etc.) vendors to determine what actions are recommended or appropriate for their particular environments.
Reporting:	All recipients of this Recommendation are required to affirm their receipt of this notice via email to alerts@nerc.com by 5:00 PM EDT on Tuesday **October 28, 2008**. Additional reporting requirements are expected and will be communicated in a supplemental notice from NERC.
Background:	Microsoft has released an out-of-band security bulletin addressing a vulnerability in the ‘RPC’ component of the Server Service and Browser Service, which may allow a remote attacker to execute arbitrary code on an effected server. Microsoft has not issued an out-of-band security bulletin in several years. A patch is available from Microsoft, as are other mitigation recommendations. Intrusion detection system and anti-virus signatures are either in development or released. Reports of an active exploit have been reported. Exploit code has been reported as readily available. The vulnerability may allow a remote unauthenticated user to execute arbitrary code on Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems. Windows Vista and Windows Server 2008 are also vulnerable to the exploit, but require the attacker to be authenticated.

Background: (continued)

The vulnerable RPC component service is used by both OPC and DCOM, which in turn are widely deployed in control system uses of Microsoft products. Exploited code may execute with System privileges.

Additional information from Microsoft, including patch availability and mitigation steps is available from: http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx and http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx.

This vulnerability has been assigned the following identifiers:
CVE/NVD ID: CVE-2008-4250: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
US-CERT Vulnerability Note VU 827267: http://www.kb.cert.org/vuls/id/827267
US-CERT Critical Infrastructure information Notice CIIN-08-297-01

There are no distribution restrictions on this Recommendation to Industry or the information contained herein.

Contact:

Scott Mix
Manager of Situation Awareness and Infrastructure Security
609.452.8060
scott.mix@nerc.net

R-2008-10-24-01