NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Recommendation to Industry

CIP: Microsoft Out-of-Band Security Bulletin MS08-067

Initial Distribution: October 24, 2008
Additional Information Distributed: November 20, 2008

Limited Exploitation of Vulnerability Has Occurred. Final Reporting Requirements Below.

Status:	**Acknowledgment of Receipt & Reporting Required By December 2, 2008.** Instructions for acknowledging reciept have been sent to the primary compliance contact.
	**PUBLIC: NO HANDLING RESTRICTIONS** More on handling >>
Instructions:	This NERC Recommendation is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Recommendation. However, pursuant to Rule 810 of NERC's Rules of Procedure, you are required to report to NERC on the status of your activities in relation to this recommendation. For U.S. entities, NERC will compile the responses and report them to the Federal Energy Regulatory Commission. Issuance of this Recommendation does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Recommendation if such failure constitutes a violation of a Reliability Standard.
Distribution:	**As posted on www.nerc.com** All Registered Entities Who else will get this alert? >> What are my responsibilities? >>
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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reporting:	Primary Compliance Contacts at Registered Entities in receipt of this notice are required to affirm their receipt of this notice and report whether they have adequately addressed this vulnerability via the online acknowledgement tool by filling out the questionnaire no later than 5:00 PM EDT on **Tuesday December 2, 2008**. Access to this tool has been provided to Primary Compliance Contacts. Those entities who are not able to affirm that they have appropriately addressed the vulnerability will be given further reporting instructions in the online questionnaire. Respondents will need the following information to complete the questionnaire: NERC Compliance Registry ID Number, Registered Entity Name, Primary Compliance Contact Contact Information. Respondents will also need to respond whether or not their organization has appropriately addressed this vulnerability and certify that an officer of the company has approved their response.
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. Exploit code has been reported as readily available, but limited exploitation of vulnerability has occurred. 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. 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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Contact:	Scott Mix Manager of Situation Awareness and Infrastructure Security 215.853.8204 scott.mix@nerc.net

R-2008-10- 24-01

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton , NJ 08540
609.452.8060 | www.nerc.com