NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Advisory

CIP: Control Microsystems ClearSCADA, ClearSCADA Prime and SCX Vulnerabilities

Initial Distribution: February 19, 2009

The vulnerabilities have not been publicly disclosed.

Why am I receiving this? >>
About NERC Alerts >>

Status:	**No Reporting is Required – For Information Only**
🟩 🟨 🟥 ⬛	**Public: No Restrictions** **More on handling >>**
Instructions:	NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. No particular response is necessary. This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory 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 Advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Initial Distribution: Primary Compliance Contacts** Transmission Owners, Transmission Operators, Load Serving Entities, Distribution Providers **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	SCADA, Operations, Planning, IT Security; and users of Control Microsystems ClearSCADA, ClearSCADA Prime and SCX.
Advisory:	A directory traversal vulnerability has been identified in the Control Microsystems ClearSCADA, ClearSCADA Prime and SCX applications. An attacker can discover directory structure and download arbitrary files from the web server with a potential for follow up attacks. During the initial attack password files can be obtained and cracked offline to discover usernames and passwords, which can elevate the attack to enable arbitrary code execution. A patch has been developed and released by Control Microsystems.

Advisory: (continued)

Mitigations:

Users of the applications should contact the vendor to obtain a copy of the patched versions of the applications using the following communications mechanism supplied by Control Microsystems Inc:

For ClearSCADA and ClearSCADA Prime:

Versions ClearSCADA 2007 R1.3, ClearSCADA Prime 2007 R1.3, ClearSCADA 2009 R1.2 and ClearSCADA Prime 2009 R1.2.
Download available: http://controlmicrosystems.com/resources-2/downloads/software-downloads/

For ClearSCADA 2007 R0.2:

Available by request only: scadacare@controlmicrosystems.com

For SCX product:

Available from Serck Controls by request only. Users are advised to contact their local Serck office for download locations from http://www.serckcontrols.com/global.html

The ES-ISAC estimates that the risk to bulk power system reliability from this vulnerability is LOW because there is no evidence of exploitation code being released into the public and there is very limited deployment in the electricity sector where the software is typically used in substation automation.

Background:

US-CERT notified the ES-ISAC of these vulnerabilities on February 18, 2009, and the information has remained undisclosed to the public. The vendor has informed its customers of these vulnerabilities, developed a patch, and has made the patch available.

More information on the subject of ‘directory’ or ‘path’ traversal can be found here:

http://cwe.mitre.org/data/definitions/22.html
http://www.owasp.org/index.php/Path_Traversal

Contact:

Doug Newbauer
Manager of Alerts
609.937.3413
doug.newbauer@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com

You have received this message because you are listed as the designated contact for your organization on the North American Electric Reliability Corporation's compliance registry. If believe you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Chris Scheetz at NERC by calling 609.452.8060 or emailing Chris directly at: chris.scheetz@nerc.net.

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