NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

CIP: OSIsoft PI Enterprise Server Authentication

Initial Distribution: October 2, 2009

Public disclosure of a control system vulnerability.

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:	**Primary Send: Primary Compliance Contacts** Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Balancing Authorities, Reliability Coordinators, Load Serving Entities, Distribution Providers **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	SCADA, EMS, Operations, Planning, IT Security, Users of OSIsoft PI Enterprise Server
Advisory:	The ES-ISAC has received information from a leading SCADA security researcher regarding a vulnerability in the authentication process of the OSIsoft PI Enterprise Server. This vulnerability may allow a remote attacker to gain access to the PI Server databases, which could allow the attacker to gain access to confidential operational information, tamper with sensitive data, and attempt to find additional vulnerabilities in the server to carry out the "corporate network to control center" attack vector. All versions of the PI Enterprise Server when configured for PI password authentication (also referred to as "explicit logins") are potentially affected. The most recent release of the PI Enterprise Server, version 3.4.380, comes with complete remediation by eliminating the requirement for PI user accounts and by adding server policy enforcement to disable explicit logins. No patch is available for prior PI Enterprise Server versions, mitigating configuration steps are described below. The ES-ISAC and ICS-CERT strongly encourage users of PI Enterprise Server configure authentication via PI Trust records, which is not affected by this vulnerability. All types of PI Trusts avoid the exchange of unsecure PI passwords. The newest PI Enterprise Server version (3.4.380) if configured with the default authentication settings is not affected by this vulnerability. It is recommended that these users verify server authentication policy is set to "explicit login disabled". The related knowledge base (KB) is available to registered users at: http://techsupport.osisoft.com/.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Advisory: (continued)	The ES-ISAC estimates that the risk to grid reliability from this vulnerability is LOW, due to no evidence of exploitation code being released into the public and the proactive approach the vendor has taken with its client base.
Background:	OSIsoft PI Enterprise Server is widely deployed across the electric sector as an industrial control system tool. The CVE is 2009-0209 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0209 .
Contact:	Doug Newbauer Alerts Manager 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 A-2009-10-02-01

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