Title: C4 SCADA Security Advisory - OSISoft PI Server Authentication Weakness

Date: September 30 2009
Author: Eyal Udassin (eyal udassin c4-security com)

Background

Vendor product information, from www.osisoft.com :
The PI System™ brings all operational data into a single system that can deliver it to users at all levels of the company - from the plant floor to the enterprise level. The PI System keeps business-critical data always online and available in a specialized time-series database by:

- Gathering event-driven data, in real-time, from multiple sources across the plant and/or enterprise
- Applying advanced analytical calculations and business rules to Contextualize and Analyze this data
- Configuring smart and thin client tools to distribute and visualize knowledge/ information to display critical operational metrics and integrate the user experience across different roles within the enterprise.

Description

Due to the sensitivity of SCADA-related vulnerabilities, we can only publicly disclose that PI Server suffers from an encryption weakness in the default authentication process.
Details of this vulnerability will be disclosed only to legitimate parties such as asset owners (utilities), after receiving the approval of the local CERT or any other local official entity.

Impact

An attacker can gain access to the PI Server databases, allowing him to:

- Gain access to confidential operational information
- Data tampering - permanent data loss or presentation of misleading decision support data
- Attempt to find additional vulnerabilities in the server to carry out the "corporate network to control center" attack vector mentioned in C4's S4 2008 paper "Control System Attack Vectors and Examples: Field Site and Corporate Network" (http://www.c4-security.com/index-5.html).

Affected Versions

PI Server - All versions

Workaround/Fix

According to the vendor, as of PI version 3.4.380.x the vulnerable authentication mechanism is deprecated, therefore no fix is planned for release for this vulnerability.
The vendor recommends the following procedures to mitigate the vulnerability:

- Enable the PI Server for Windows authentication and configure PI Trust records
- Use IPSec between the PI Server and the different client computers

Additional Information

For additional information please contact us at info_at_c4-security.com.
Note that we will respond only to verified utility personnel and governmental
agencies. Details of this vulnerability will be disclosed only to legitimate
parties such as asset owners (utilities), after receiving the approval of the
local CERT or any other local official entity.

The CVE identifier assigned to this vulnerability by CERT is CVE-2009-0209

Credit

This vulnerability was discovered and exploited by Eyal Udassin, Jonathan Afek and Yaron Budowsky from C4 Security (http://www.c4-security.com).

C4 Security is a leader in SCADA security reviews, auditing and penetration testing.