

Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5orS7

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-09/0279.html>

From: Nasir Farhat Khan (nasir@instecdigital.com)

Date: 09/29/01

Message-ID: <003101c148d7\$6408ee80\$1100a8c0@viper.pvt>

From: "Nasir Farhat Khan" <nasir@instecdigital.com>

To: <PEN-TEST@SECURITYFOCUS.COM>

Subject: Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5orS7

Date: Sat, 29 Sep 2001 16:10:46 +0500

IMPORTANT:

DO NOT TO TRY this in a production environment. PLCs are used to control production equipment (machinery) and consequences can be very dangerous and life threatening.

My apologies for repeating the warning message. Unlike the PC servers and network equipment malfunction in PLCs and control equipment can be quite devastating. Most of the time Control System networks are segregated from office network just because of this reason.

Most PLCs and their Communication processors have very little CPU memory so it would be fairly easy to do a DoS with a result that it wont be able to update the GUI with current values or it may simply go down.

In control systems "Loss of View" condition where operators are unable to view plant data is seen as a very "Critical Situation".

I checked the S5 datasheets on the internet and it seems that it does support TCP/IP and SNMP. In addition to this it also supports RS485 (which is a multidrop network and can connect to multiple nodes, including your notebook containing programming software).

Nasir

nasir@instecdigital.com

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

SecurityFocus Penetration: Re: Pen-testing Simatic Data Aquisit

- **Previous message:** Steve Gadd: "Technical Requirements"
- **In reply to:** Patrick Coomans: "Re: Pen-testing Simatic Data Aquisition Periphery e.g. PLC S5 orS7"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]