RBS-2013-003

Schneider Electric Multiple Products Modbus Serial Driver MBAP Packet Parsing Buffer Overflow

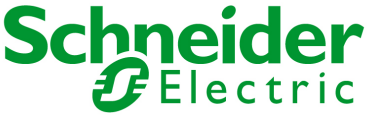


Table of Contents

About Risk Based Security

Mission

To equip clients with the technology and customized risk-based consulting solutions to turn security data into information and information into a competitive advantage.

Background

Risk Based Security, Inc., incorporated in 2011, was established to better support the users/contributors to the Open Security Foundation (OSF), with the technology to turn security data into a competitive advantage.

The OSF's wealth of historical data, combined with the interactive dashboards and analytics offered by Risk Based Security provide a first of its kind risk identification and security management tool.

Risk Based Security further complements the data analytics with risk-focused consulting services to address industry specific information security and compliance challenges.

Discriminators

Risk Based Security offers a full set of analytics and user-friendly dashboards designed specifically to identify security risks by industry.

Risk Based Security is the only company that offers its clients a fully integrated solution – real time information, analytical tools and purpose-based consulting.

Unlike other security information providers, Risk Based Security offers companies comprehensive insight into data security threats and vulnerabilities most relevant to their industry.

Vulnerable Program Details

Vendor:	Schneider Electric
Tested Product:	TwidoSuite
Tested Version:	2.31.04
Component:	ModbusDrv.exe
File version:	1.7.33.35
Tested Platform:	Windows Server 2003 R2 Enterprise Edition

Table of affected products and versions as reported by Schneider Electric[1] can be found below:

Product	**Version**
TwidoSuite	2.31.04 and prior
PowerSuite	2.6 and prior
SoMove	V1.7 and prior
SoMachine	V2.0, V3.0, V3.1, V3.0
XSUnity Pro	V7.0 and prior
UnityLoader	V2.3 and prior
Concept	V2.6 SR7 and prior
ModbusCommDTM sl	V2.1.2 and prior
PL7	V4.5 SP5 and prior
SFT2841	V14; V13.1 and prior
OFS	V3.50 and prior

[1] http://download.schneider-electric.com/files?p_File_Id=47991052&p_File_Name=SEVD-2013-070-01.pdf

Windows OS version	Modbus Serial Driver
XP 32 bit	V1.10 IE v37
Vista 32 bit	2.2 IE12
Windows 7 32 bit	2.2 IE12
Windows 7 64 bit	3.2 IE12

References

RBS: RBS-2013-003
OSVDB: 92202
CVE: To be assigned by MITRE or ICS-CERT
ICS-CERT: Advisory scheduled for patch release

Credits

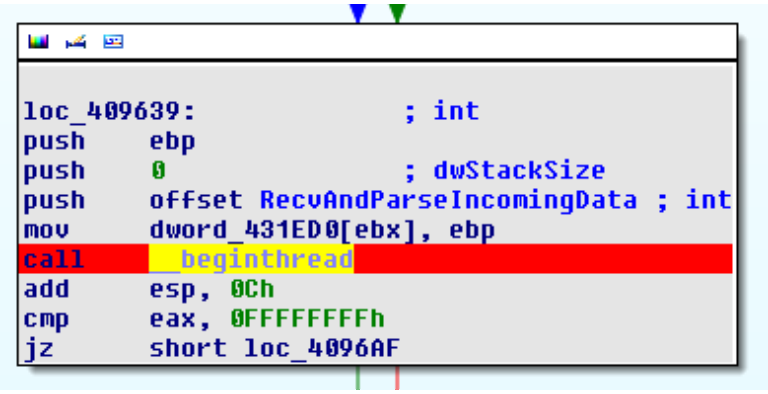
Carsten Eiram, Risk Based Security

Twitter: @CarstenEiram
Twitter: @RiskBased

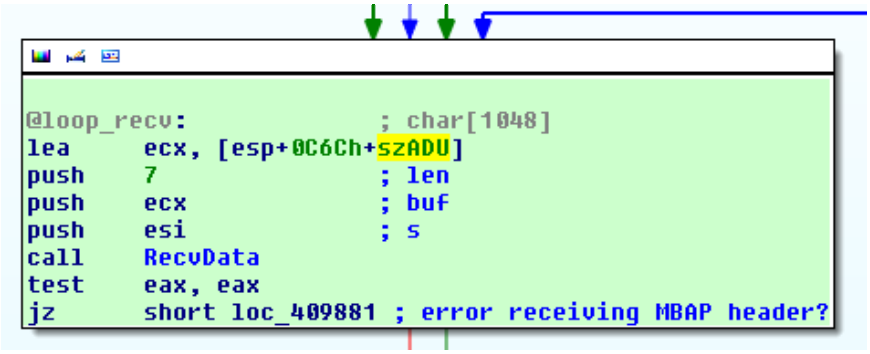
Vulnerability Details

A large number of products from Schneider Electric bundle the Schneider Modbus Serial Driver (ModbusDrv.exe). It's default state may depend on the product bundling it; in the case of TwidoSuite, it is started when attempting to connect to a controller on a serial port e.g. when in "Monitoring" mode or when opening an existing project on a controller in "Programming" mode.

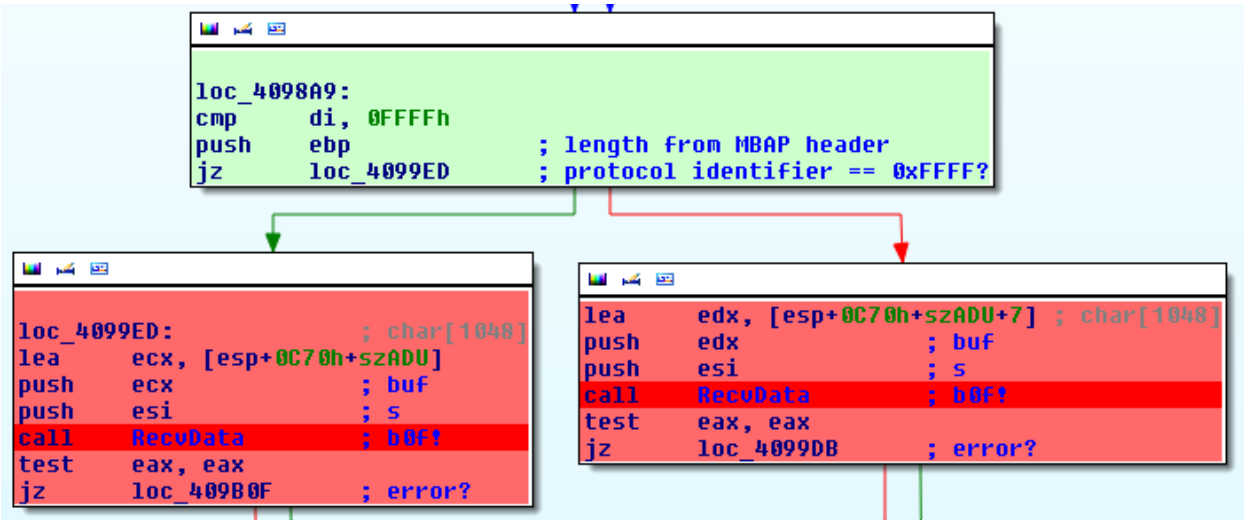
Once started, the Modbus Serial Driver binds to TCP port 27700 by default and enters a loop, waiting for connections from remote clients. Once a client connects, a new thread is created to receive and parse incoming data.



This function eventually enters a loop to receive incoming Modbus TCP/IP ADUs and starts by reading in the initial 7 bytes (MBAP header).

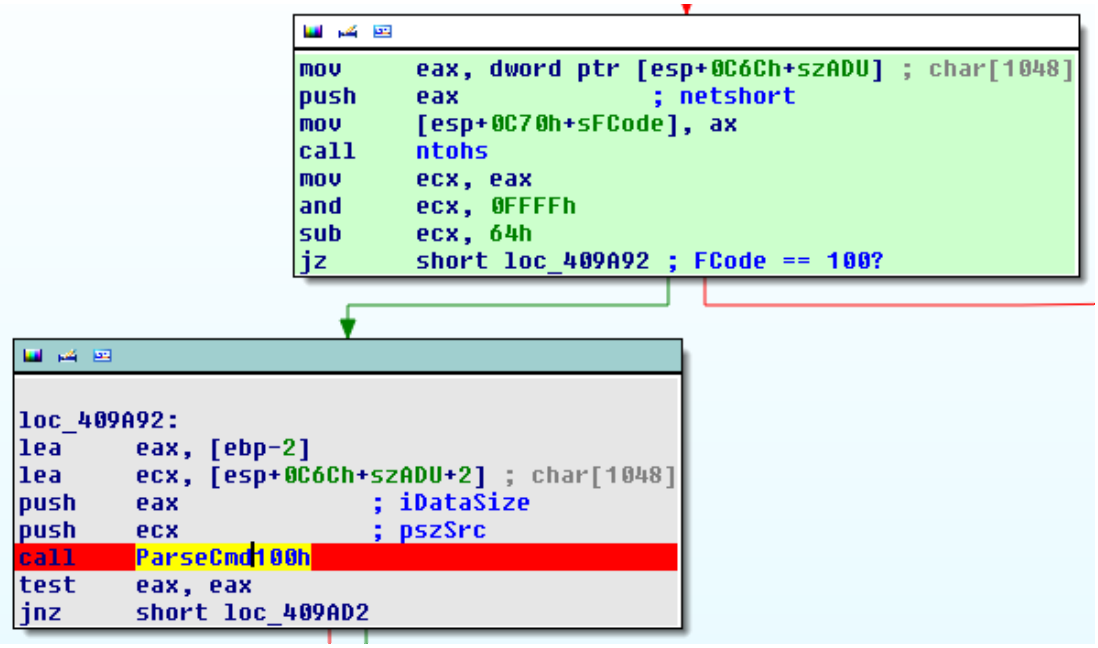


A check determines if the supplied "protocol identifier" in the MBAP header is 0xFFFF and branches accordingly. In either case, the remaining data (PDU) in the Modbus TCP/IP ADU is read from the socket into a 1048 byte stack-based buffer using the length supplied in the MBAP header as size argument without ensuring that the stack buffer is adequately sized. This may result in stack-based buffer overflows.

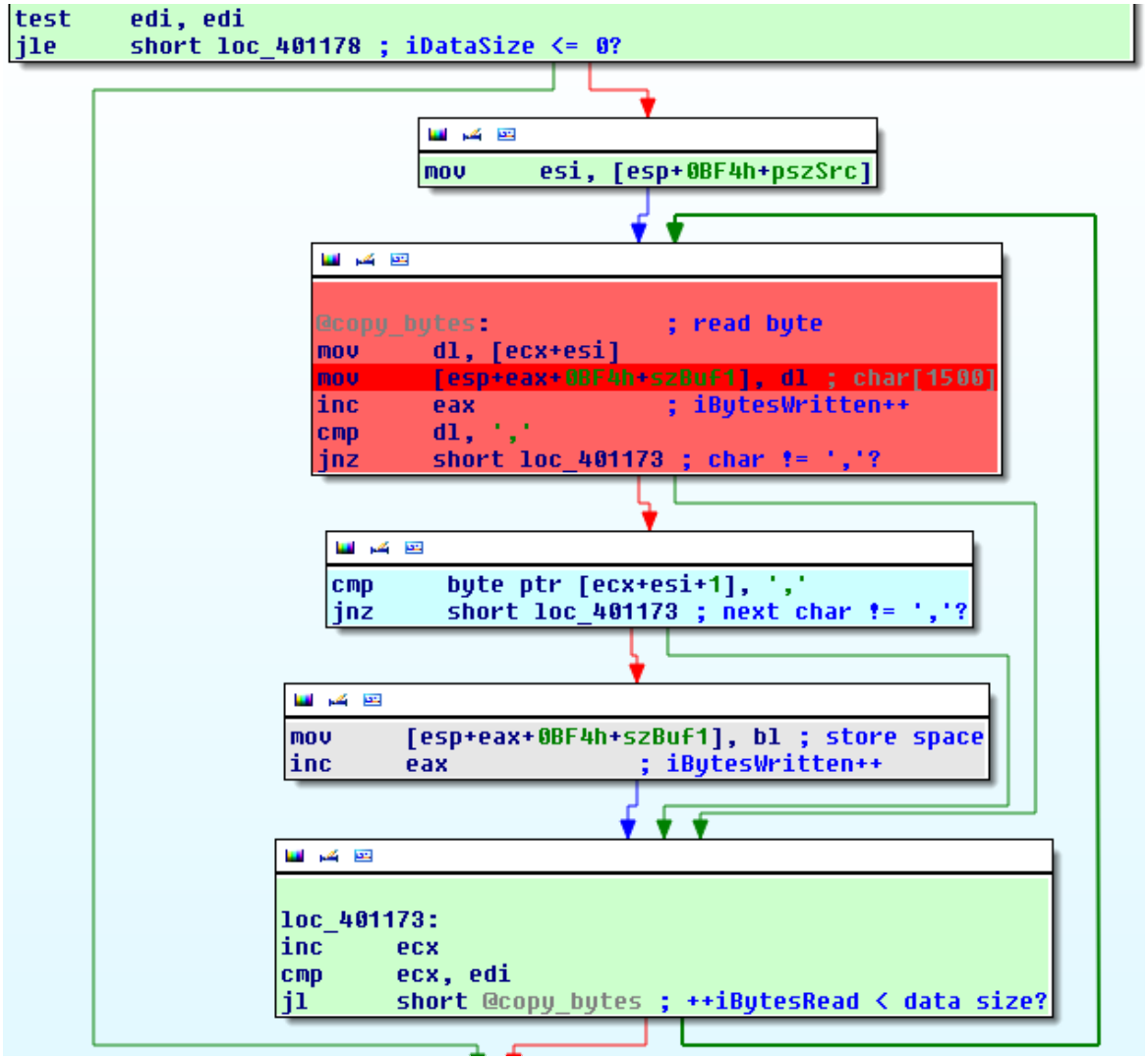


These buffer overflows can, however, not immediately be exploited to gain control of the program flow by e.g. overwriting the return address, as the function is running as a separate thread and terminates once reaching its end. Instead, the vulnerabilities have to be chained with other problems in the code in order to trigger an exploitable condition.

One way of achieving this is by setting the "protocol identifier" in the MBAP header to 0xFFFF and the "function code" of the following data to 64h (i.e. function code 100). This causes a function to be called to specifically parse the received function code 100 message.



Within this function the data is copied within a loop into a 1500 byte stack buffer based on the supplied data size without performing any bounds checks.



As a buffer overflow could previously have occurred, and this copy operation neglects to properly perform boundary checks, another stack-based buffer overflow can be triggered here, where the function's return address can be successfully overwritten and used to gain control of the program flow, as no stack cookies are implemented.

An attacker can exploit this to execute arbitrary code with the privileges of the user running the service.

Solution

Patched component: N/A
Patched file version: N/A

Schneider Electric published an advisory to alert customers prior to fixes being ready. Though Risk Based Security was prepared to postpone disclosure until fixes were developed, the amount of detail in the vendor's advisory about affected products and components was deemed sufficient for an attacker to relatively quickly find and exploit the vulnerability.

As a result, Risk Based Security is now publishing this analysis even though patches or updated versions are not available. This is done to ensure that users of these products are fully aware of the threat, its impact, can detect attacks, and work around it until fixes are available.

Timeline

2013/01/05	Vulnerability discovered.
2013/01/08	Vulnerability reported to ICS-CERT.
2013/01/24	Vulnerability acknowledged by Schneider Electric.
2013/03/11	Vendor publishes security notification prior to fixes being ready.
2013/03/13	ICS-CERT provides status update.
2013/04/10	Alerts published for OSVDB and RBS VulnDB Service[2]
2013/05/06	Publication of this vulnerability report.

[2] http://www.riskbasedsecurity.com/risk-data-analytics/vulnerability-database/