Getting security objectives wrong

A cautionary tale of an Industrial Control System

Simon Foley
NTNU IIK Gjøvik
mailto:simon.foley@ntnu.no

17 September, 2019

Getting security objectives wrong

A cautionary tale of an Industrial Control System

Simon Foley
NTNU IIK Gjøvik
mailto:simon.foley@ntnu.no

Software can be chaotic, but we make it work
Expert
Trying Stuff Until it Works
O RLY?
The Practical Developer
@ThePracticalDev

17 September, 2019

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

TCP/IP Recap

[IP] A source system wants to send a message to a destination system.

$$\text{Msg 1}: \quad \mathit{Source} \rightarrow \mathit{Destination}: \quad \mathit{message}$$

The IP-address of the source and destination are contained in the Network header of the packets exchanged. The message data is contained in the application header.

However, when multiple messages are sent it is possible that they may arrive at the destination out-of-sequence or are even lost.

[TCP] facilitates correct ordering of data arriving reliably at destination socket connection.

Source system establishes a TCP connection to a port on a destination system, whereupon the source can send any amount of data and be sure that the destination application (associated with that port) receives the data in the correct order.

Network Application Example

For example, `sendmail` is a Unix application that is used to route, send and receive email messages. It runs on a server, ‘listening’ on Port 25 for requests from other systems.

For example, a user on on `cosmos.ucc.ie` sends a request to the application running on `smtp.ucc.ie`:

```
> telnet smtp.ucc.ie 25
helo cosmos.ucc.ie
mail from: <taoiseach@gov.ie>
rcpt to: <s.foley@cs.ucc.ie>
data
......
```

The data related to the request (above) is contained within the application data of the packet.

Application does not provide authentication of sender: no check whether user/system sending request corresponds to originating email address.

Network Application Example

Inspecting packet sent from `cosmos.ucc.ie` to Port 25 on `smtp.cs.ucc.ie`, yields the following data (organized by header):

Physical	HWaddr (cosmos) 00:10:5A:4B:09:32, ...
Network	from 143.239.75.206 to 143.239.153.184 ...
Transport	... to port 25, ...

Application	`mail from: <taoiseach@gov.ie>`
	`rcpt to: <s.foley@cs.ucc.ie>`
	`data`
	......

When the packet arrives at `smtp.ucc.ie`, a daemon, such as xinetd in Unix, knows that a packet arriving on Port 25 should be directed to the `sendmail` process. The `sendmail` process running on `smtp.ucc.ie` effectively receives the application data portion of this packet.

`sendmail` implements the SMTP protocol (an "application layer protocol").

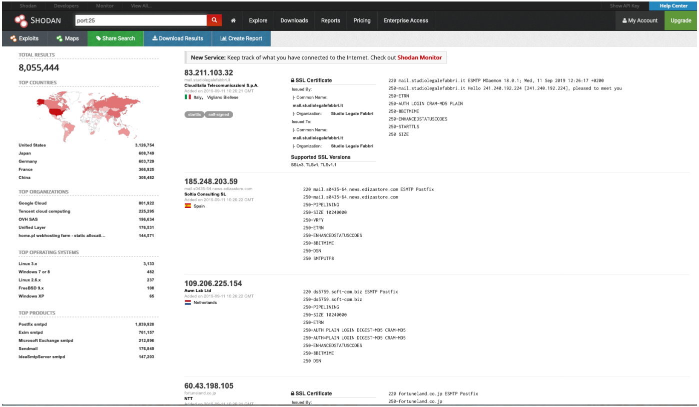
Sample Network Packet Content

`tcpdump -A` display traffic on a network (run here on `smtp.cs.ucc.ie`)

```
sudo tcpdump -A port smtp
[....]
09:25:45.143837 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 1:21(20) ack 35 win 65535 <nop,nop,timestamp 157409668 291916037>
    U.......w.....J......3......a...fI.helo cosmos.ucc.ie
[...]
09:25:45.144090 IP neptune.cs.ucc.ie.smtp > 143.239.74.165.50483:
    P 35:55(20) ack 21 win 5792 <nop,nop,timestamp 291932278 157409668>
    U.................J....3.f.va..250 neptune.ucc.ie
[...]
09:26:23.078507 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 21:48(27) ack 55 win 65535 <nop,nop,timestamp 157410047 291932278>
    U.......~.....J......3......a...f.vmail from: <taoiseach@gov.ie>
[...]
09:26:44.486250 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 48:77(29) ack 69 win 65535 <nop,nop,timestamp 157410261 291970212>
    U.............J......3.....a...g..rcpt to <s.foley@cs.ucc.ie>
```

Shodan

Searching for sites based on Internet header data



New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

TOTAL RESULTS

8,055,444

TOP COUNTRIES

United States	3,126,754
Japan	608,749
Germany	603,729
France	366,925
China	308,482

TOP ORGANIZATIONS

Google Cloud	801,922
Tencent cloud computing	225,295
OVH SAS	196,634
Unified Layer	176,531
home.pl webhosting farm - static allocati...	144,571

TOP OPERATING SYSTEMS

Linux 3.x	3,133
Windows 7 or 8	482
Linux 2.6.x	237
FreeBSD 9.x	108
Windows XP	65

TOP PRODUCTS

Postfix smtpd	1,839,920
Exim smtpd	761,157
Microsoft Exchange smtpd	212,896
Sendmail	176,849
IdeaSmtpServer smtpd	147,203

83.211.103.32
mail.studiolegalefabbri.it
Clouditalia Telecomunicazioni S.p.A.
Added on 2019-09-11 10:26:21 GMT
Italy, Vigliano Biellese

SSL Certificate
Issued By:
|- Common Name: **mail.studiolegalefabbri.it**
|- Organization: **Studio Legale Fabbri**
Issued To:
|- Common Name: **mail.studiolegalefabbri.it**
|- Organization: **Studio Legale Fabbri**

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1

```
220 mail.studiolegalefabbri.it ESMTP MDaemon 18.0.1; Wed, 11 Sep 2019 12:26:17 +0200
250-mail.studiolegalefabbri.it Hello 241.240.192.224 [241.240.192.224], pleased to meet you
250-ETRN
250-AUTH LOGIN CRAM-MD5 PLAIN
250-8BITMIME
250-ENHANCEDSTATUSCODES
250-STARTTLS
250 SIZE
```

185.248.203.59
mail.s0435-64.news.edizastore.com
Soltia Consulting SL
Added on 2019-09-11 10:26:22 GMT
Spain

```
220 mail.s0435-64.news.edizastore.com ESMTP Postfix
250-mail.s0435-64.news.edizastore.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
```

109.206.225.154
Awm Lab Ltd
Added on 2019-09-11 10:26:22 GMT
Netherlands

```
220 ds5759.soft-com.biz ESMTP Postfix
250-ds5759.soft-com.biz
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5
250-AUTH=PLAIN LOGIN DIGEST-MD5 CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

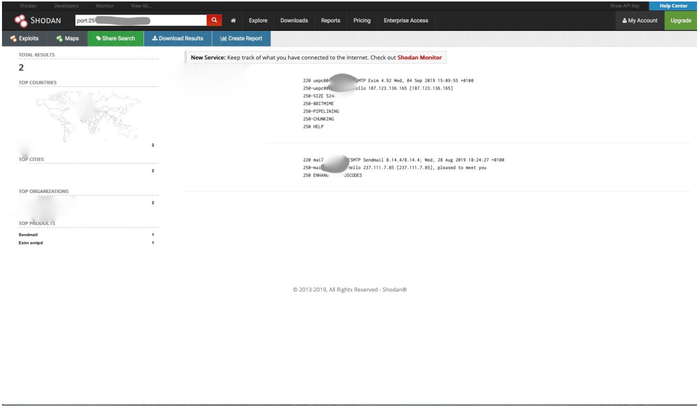
60.43.198.105
fortuneland.co.jp
NTT
Added on 2019-09-11 10:26:21 GMT

SSL Certificate
Issued By:

```
220 fortuneland.co.jp ESMTP Postfix
250-fortuneland.co.jp
```

Shodan

Searching for sites based on Internet header data



TOTAL RESULTS

2

TOP COUNTRIES

[redacted] 2

TOP CITIES

[redacted] 2

TOP ORGANIZATIONS

[redacted] 2

TOP PRODUCTS

Sendmail	1
Exim smtpd	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

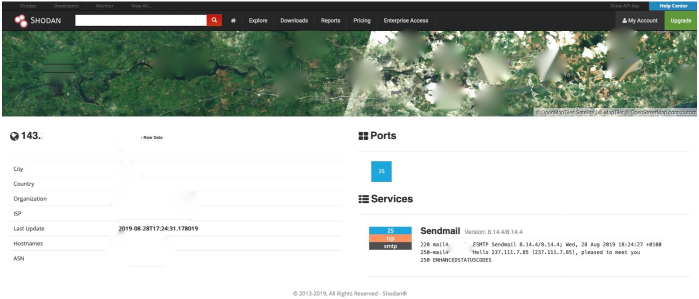
```
220 uepc00[redacted]MTP Exim 4.92 Wed, 04 Sep 2019 15:09:55 +0100
250-uepc00[redacted]ello 187.123.136.165 [187.123.136.165]
250-SIZE 524[redacted]
250-8BITMIME
250-PIPELINING
250-CHUNKING
250 HELP
```

```
220 mail[redacted]ESMTP Sendmail 8.14.4/8.14.4; Wed, 28 Aug 2019 18:24:27 +0100
250-mai[redacted]Hello 237.111.7.85 [237.111.7.85], pleased to meet you
250 ENHANC[redacted]USCODES
```

© 2013-2019, All Rights Reserved - Shodan®

Shodan

Searching for sites based on Internet header data



143.

/ Raw Data

City	
Country	
Organization	
ISP	
Last Update	2019-08-28T17:24:31.178019
Hostnames	
ASN	

Ports

25

Services

25 tcp smtp

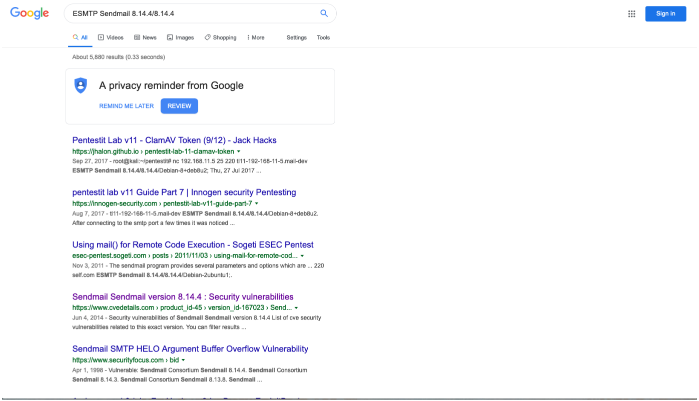
Sendmail Version: 8.14.4/8.14.4

```
220 mail4          ESMTP Sendmail 8.14.4/8.14.4; Wed, 28 Aug 2019 18:24:27 +0100
250-mail4          Hello 237.111.7.85 [237.111.7.85], pleased to meet you
250 ENHANCEDSTATUSCODES
```

© 2013-2019, All Rights Reserved - Shodan®

Shodan

Searching for sites based on Internet header data



About 5,880 results (0.33 seconds)

A privacy reminder from Google

Pentestit Lab v11 - ClamAV Token (9/12) - Jack Hacks
https://jhalon.github.io › pentestit-lab-11-clamav-token
Sep 27, 2017 - root@kali:~/pentestit# nc 192.168.11.5 25 220 tl11-192-168-11-5.mail-dev **ESMTP Sendmail 8.14.4/8.14.4**/Debian-8+deb8u2; Thu, 27 Jul 2017 ...

pentestit lab v11 Guide Part 7 | Innogen security Pentesting
https://innogen-security.com › pentestit-lab-v11-guide-part-7
Aug 7, 2017 - tl11-192-168-11-5.mail-dev **ESMTP Sendmail 8.14.4/8.14.4**/Debian-8+deb8u2. After connecting to the smtp port a few times it was noticed ...

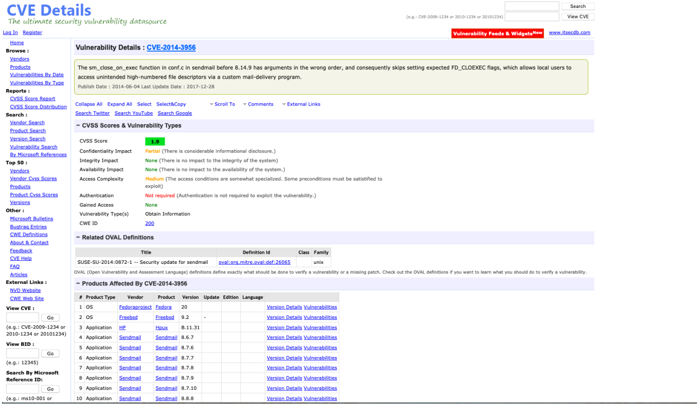
Using mail() for Remote Code Execution - Sogeti ESEC Pentest
esec-pentest.sogeti.com › posts › 2011/11/03 › using-mail-for-remote-cod...
Nov 3, 2011 - The sendmail program provides several parameters and options which are ... 220 self.com **ESMTP Sendmail 8.14.4/8.14.4**/Debian-2ubuntu1;.

Sendmail Sendmail version 8.14.4 : Security vulnerabilities
https://www.cvedetails.com › product_id-45 › version_id-167023 › Send...
Jun 4, 2014 - Security vulnerabilities of **Sendmail Sendmail** version 8.14.4 List of cve security vulnerabilities related to this exact version. You can filter results ...

Sendmail SMTP HELO Argument Buffer Overflow Vulnerability
https://www.securityfocus.com › bid
Apr 1, 1998 - Vulnerable: **Sendmail** Consortium **Sendmail** 8.14.4. **Sendmail** Consortium **Sendmail** 8.14.3. **Sendmail** Consortium **Sendmail** 8.13.8. **Sendmail** ...

Shodan

Searching for sites based on Internet header data



CVE Details
The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home
Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website
- CWE Web Site

View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :
Go
(e.g.: 12345)

Search By Microsoft Reference ID:
Go
(e.g.: ms10-001 or

Vulnerability Details : CVE-2014-3956

The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.
Publish Date : 2014-06-04 Last Update Date : 2017-12-28

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

− CVSS Scores & Vulnerability Types

CVSS Score	1.9
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

− Related OVAL Definitions

Title	Definition Id	Class	Family
SUSE-SU-2014:0872-1 -- Security update for sendmail	oval:org.mitre.oval:def:26065		unix

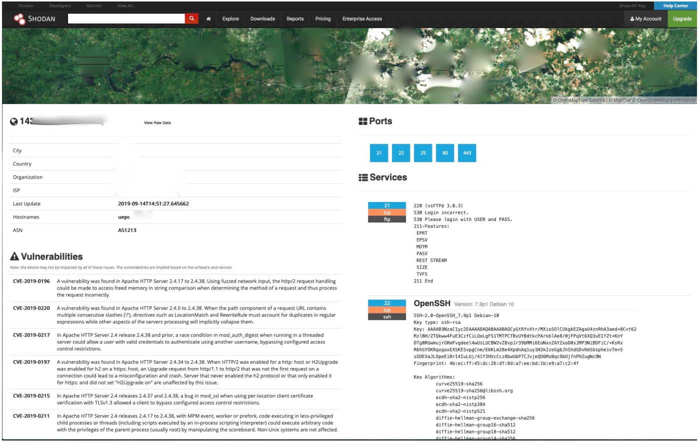
OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

− Products Affected By CVE-2014-3956

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Fedoraproject	Fedora	20				Version Details Vulnerabilities
2	OS	Freebsd	Freebsd	9.2	-			Version Details Vulnerabilities
3	Application	HP	Hpux	B.11.31				Version Details Vulnerabilities
4	Application	Sendmail	Sendmail	8.6.7				Version Details Vulnerabilities
5	Application	Sendmail	Sendmail	8.7.6				Version Details Vulnerabilities
6	Application	Sendmail	Sendmail	8.7.7				Version Details Vulnerabilities
7	Application	Sendmail	Sendmail	8.7.8				Version Details Vulnerabilities
8	Application	Sendmail	Sendmail	8.7.9				Version Details Vulnerabilities
9	Application	Sendmail	Sendmail	8.7.10				Version Details Vulnerabilities
10	Application	Sendmail	Sendmail	8.8.8				Version Details Vulnerabilities

Shodan

Searching for sites based on Internet header data



14[redacted]

City	[redacted]
Country	[redacted]
Organization	[redacted]
ISP	[redacted]
Last Update	2019-09-14T14:51:27.645662
Hostnames	uepc[redacted]
ASN	AS1213

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Ports

21 22 25 80 443

Services

21
tcp
ftp

```
220 (vsFTPd 3.0.3)
530 Login incorrect.
530 Please login with USER and PASS.
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
```

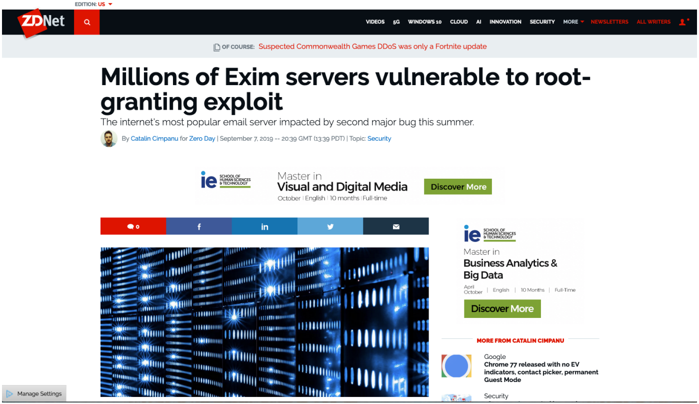
22
tcp
ssh

OpenSSH Version: 7.9p1 Debian 10

```
SSH-2.0-OpenSSH_7.9p1 Debian-10
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCyGtRYvXtr/MXioSOlCUkgkEZAgaU4znRhA3aed+8Cvt62
MzlBH/ZTQkww4FuE3CzfCiLQoLgFS1TMTPCTBvUYBdtkcPArkblAe8/0jFPqVt6XQ3uEIfZt+KnY
DTg0RUwmujrGRmFvgdeel4wUsLUCBW2vZ8vpJr39bMMi6EoNxnZAYZxoD0sJMP3NiBDFiC/+KsRx
R6hGYOKRqxgoxEXSKESvpgCnm/E6KLm28e4XpdnAq1uy1N3k2zeGgbJhShdGDvRmSbspheivTm+5
sGDEVaJLOpeEiBrI4IuLUj/41Y3HVcCcz8bwUbP7CJvjeQD6MxBqc9bOjfnPHZugNc9N
Fingerprint: 4b:ec:ff:45:dc:26:df:8d:a7:ee:bd:1b:e9:a7:c2:4f

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
```

Shodan

Searching for sites based on Internet header data


EDITION: US
ZDNet
VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

OF COURSE: Suspected Commonwealth Games DDoS was only a Fortnite update

Millions of Exim servers vulnerable to root-granting exploit

The internet's most popular email server impacted by second major bug this summer.

By Catalin Cimpanu for Zero Day | September 7, 2019 -- 20:39 GMT (13:39 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

Google
Chrome 77 released with no EV indicators, contact picker, permanent Guest Mode

Security

Outline of Talk

Networking recap

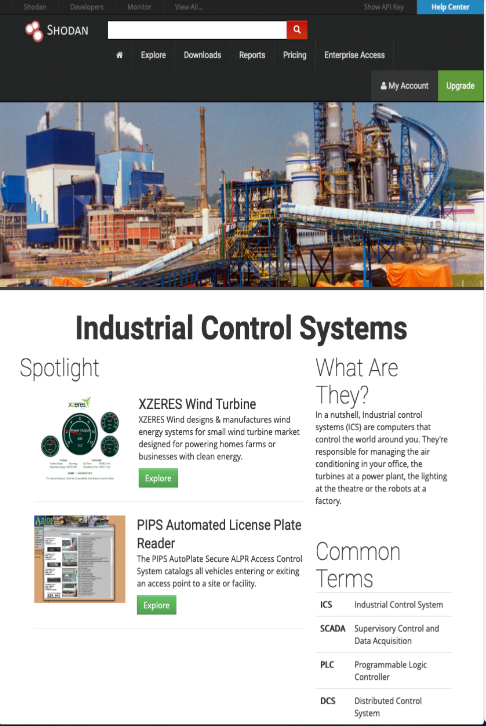
Motivation

The cautionary tale

Threat Management

Conclusion

Extra



Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

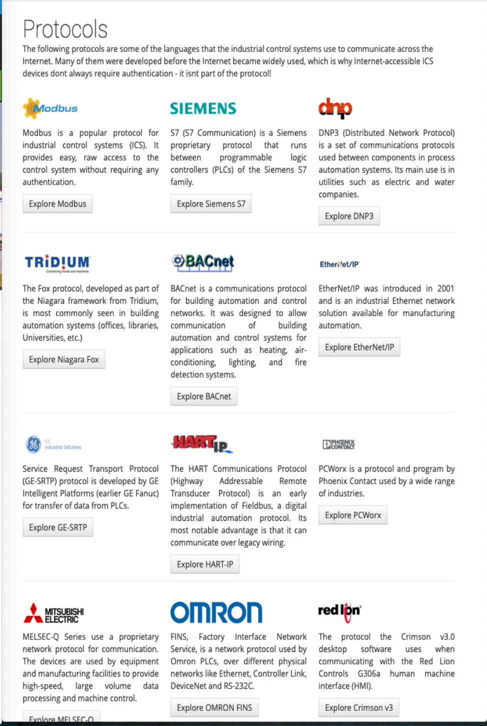
Explore

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System



Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

Explore HART-IP

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

Explore MELSEC-Q

FINS, Factory Interface Network Service, is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

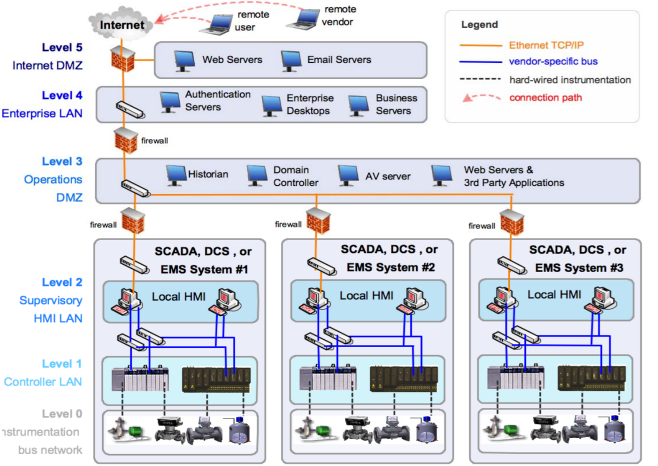
Explore OMRON FINS

The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G306a human machine interface (HMI).

Explore Crimson v3

SCADA / Industrial Control Systems

Supervisory Control and Data Acquisition

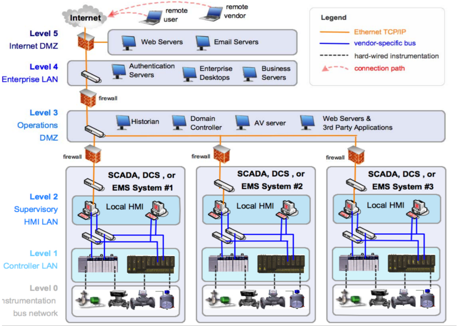


SCADA over public networks

One seemingly simple security objective

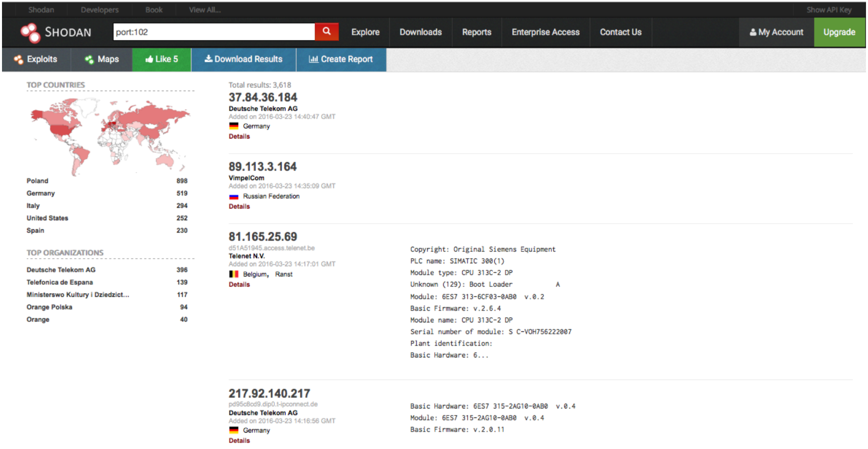
"[...] SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks. [...]"

[*Securing the move to IP-based SCADA/PLC networks*, UK Centre for the Protection of National Infrastructure (CPNI), 2011]



Use shodan to search for a use case

Siemens S7comm protocol over TCP/TSAP on Port 102



TOP COUNTRIES

Poland	898
Germany	519
Italy	294
United States	252
Spain	230

TOP ORGANIZATIONS

Deutsche Telekom AG	396
Telefonica de Espana	139
Ministerswo Kultury i Dziedzict...	117
Orange Polska	94
Orange	40

Total results: 3,618

37.84.36.184
Deutsche Telekom AG
Added on 2016-03-23 14:40:47 GMT
Germany
Details

89.113.3.164
VimpelCom
Added on 2016-03-23 14:35:09 GMT
Russian Federation
Details

81.165.25.69
d51A51945.access.telenet.be
Telenet N.V.
Added on 2016-03-23 14:17:01 GMT
Belgium, Ranst
Details

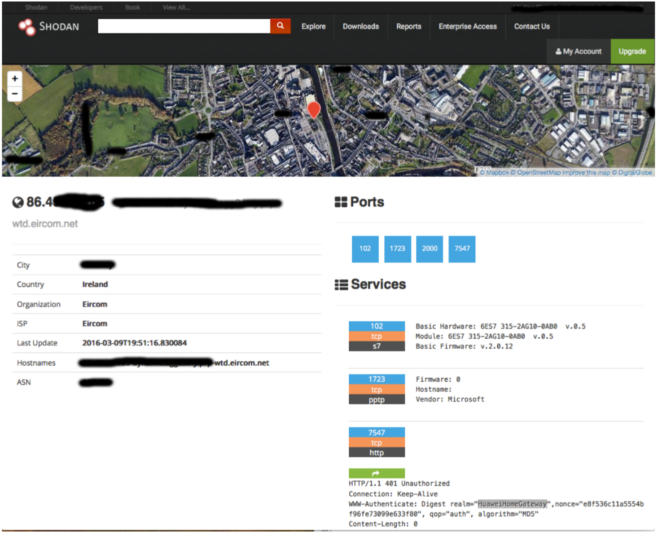
```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 313C-2 DP
Unknown (129): Boot Loader           A
Module: 6ES7 313-6CF03-0AB0  v.0.2
Basic Firmware: v.2.6.4
Module name: CPU 313C-2 DP
Serial number of module: S C-VOH756222007
Plant identification:
Basic Hardware: 6...
```

217.92.140.217
pd95c8cd9.dip0.t-ipconnect.de
Deutsche Telekom AG
Added on 2016-03-23 14:16:56 GMT
Germany
Details

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.4
Module: 6ES7 315-2AG10-0AB0  v.0.4
Basic Firmware: v.2.0.11
```

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102



86.4[redacted] [redacted]

wtd.eircom.net

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-03-09T19:51:16.830084
Hostnames	[redacted]-wtd.eircom.net
ASN	[redacted]

Ports

102 1723 2000 7547

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

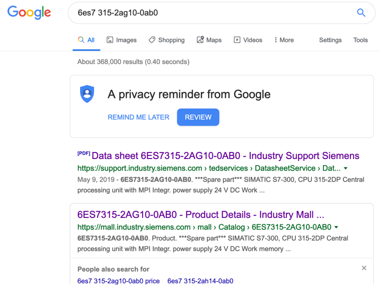
1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

What have we found?



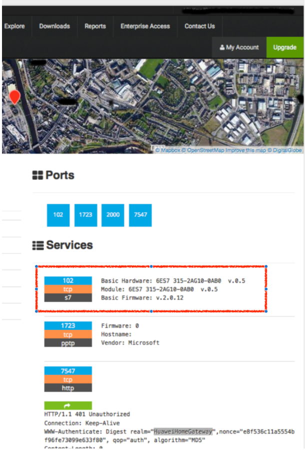
About 368,000 results (0.40 seconds)

A privacy reminder from Google

[PDF] Data sheet 6ES7315-2AG10-0AB0 - Industry Support Siemens
https://support.industry.siemens.com › tedservices › DatasheetService › Dat...
May 9, 2019 - **6ES7315-2AG10-0AB0**. ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work ...

6ES7315-2AG10-0AB0 - Product Details - Industry Mall ...
https://mall.industry.siemens.com › mall › Catalog › 6ES7315-2AG10-0AB0
6ES7315-2AG10-0AB0. Product. ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work memory ...

People also search for
6es7 315-2ag10-0ab0 price 6es7 315-2ah14-0ab0



[redacted]

[redacted]

Ports

102 1723 2000 7547

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

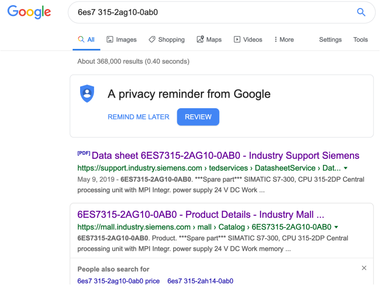
1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

What have we found?



Google

6es7 315-2ag10-0ab0

About 368,000 results (0.40 seconds)

A privacy reminder from Google

[PDF] Data sheet 6ES7315-2AG10-0AB0 - Industry Support Siemens

https://support.industry.siemens.com › tedservices › DatasheetService › Dat... ▾

May 9, 2019 - **6ES7315-2AG10-0AB0**. ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work ...

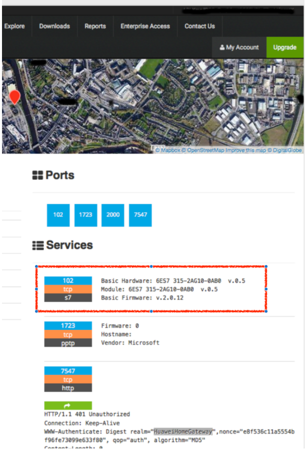
6ES7315-2AG10-0AB0 - Product Details - Industry Mall ...

https://mall.industry.siemens.com › mall › Catalog › 6ES7315-2AG10-0AB0 ▾

6ES7315-2AG10-0AB0. Product. ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work memory ...

People also search for

6es7 315-2ag10-0ab0 price 6es7 315-2ah14-0ab0



[redacted]

[redacted]

Ports

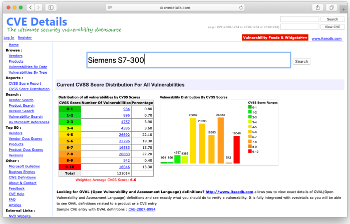
102 1723 2000 7547

Services

```
102   Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
tcp   Module: 6ES7 315-2AG10-0AB0  v.0.5
s7    Basic Firmware: v.2.0.12

1723  Firmware: 0
tcp   Hostname:
pptp  Vendor: Microsoft

7547
tcp
http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details



Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	934	0.80
1-2	896	0.70
2-3	4757	3.90
3-4	4385	3.60
4-5	26692	22.10
5-6	23296	19.30
6-7	16583	13.70
7-8	26883	22.20
8-9	542	0.40
9-10	16046	13.30
Total	121014	

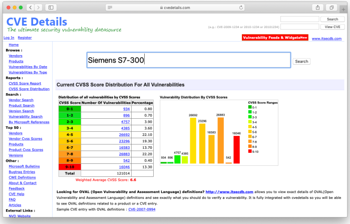
Weighted Average CVSS Score: **6.6**

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.

Sample CVE entry with OVAL definitions : CVE-2007-0994

Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website

Siemens S7-300

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

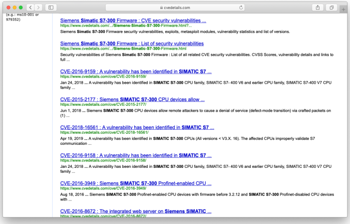
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	934	0.80
1-2	896	0.70
2-3	4757	3.90
3-4	4385	3.60
4-5	26692	22.10
5-6	23296	19.30
6-7	16583	13.70
7-8	26883	22.20
8-9	542	0.40
9-10	16046	13.30
Total	121014	

Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.

Sample CVE entry with OVAL definitions : CVE-2007-0994



(e.g.: ms10-001 or 979352)

Siemens **Simatic S7-300** Firmware : CVE security vulnerabilities ...
https://www.cvedetails.com/.../**Siemens-Simatic-S7-300**-Firmware.html?...
Siemens **Simatic S7-300** Firmware security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Siemens **Simatic S7-300** Firmware : List of security vulnerabilities
https://www.cvedetails.com/.../**Siemens-Simatic-S7-300**-Firmware.html
Security vulnerabilities of Siemens **Simatic S7-300** Firmware : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full ...

CVE-2016-9159 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2016-9159/
Jan 24, 2018 ... A vulnerability has been identified in **SIMATIC S7-300** CPU family, SIMATIC S7- 400 V6 and earlier CPU family, SIMATIC S7-400 V7 CPU family ...

CVE-2015-2177 : Siemens **SIMATIC S7-300** CPU devices allow ...
https://www.cvedetails.com/cve/CVE-2015-2177/
Jun 1, 2018 ... Siemens **SIMATIC S7-300** CPU devices allow remote attackers to cause a denial of service (defect-mode transition) via crafted packets on (1) ...

CVE-2018-16561 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2018-16561/
Apr 19, 2019 ... A vulnerability has been identified in **SIMATIC S7-300** CPUs (All versions < V3.X. 16). The affected CPUs improperly validate S7 communication ...

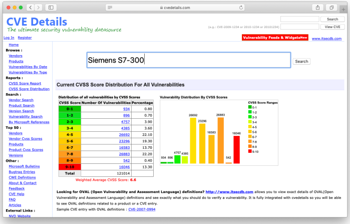
CVE-2016-9158 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2016-9158/
Jan 24, 2018 ... A vulnerability has been identified in **SIMATIC S7-300** CPU family, SIMATIC S7- 400 V6 and earlier CPU family, SIMATIC S7-400 V7 CPU family ...

CVE-2016-3949 : Siemens **SIMATIC S7-300** Profinet-enabled CPU ...
https://www.cvedetails.com/cve/CVE-2016-3949/
Aug 18, 2016 ... Siemens **SIMATIC S7-300** Profinet-enabled CPU devices with firmware before 3.2.12 and **SIMATIC S7-300** Profinet-disabled CPU devices with ...

CVE-2016-8672 : The integrated web server on **Siemens SIMATIC** ...
https://www.cvedetails.com/cve/CVE-2016-8672/

Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details



Current CVSS Score Distribution For All Vulnerabilities

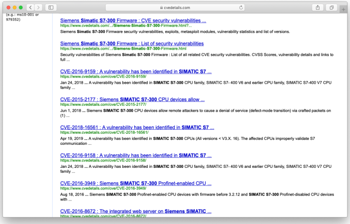
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	934	0.80
1-2	896	0.70
2-3	4757	3.90
3-4	4385	3.60
4-5	26692	22.10
5-6	23296	19.30
6-7	16583	13.70
7-8	26883	22.20
8-9	542	0.40
9-10	16046	13.30
Total	121014	

Weighted Average CVSS Score: 6.6

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.

Sample CVE entry with OVAL definitions : CVE-2007-0994



Siemens **Simatic S7-300** Firmware : CVE security vulnerabilities ...
https://www.cvedetails.com/.../**Siemens-Simatic-S7-300**-Firmware.html?...
Siemens **Simatic S7-300** Firmware security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Siemens **Simatic S7-300** Firmware : List of security vulnerabilities
https://www.cvedetails.com/.../**Siemens-Simatic-S7-300**-Firmware.html
Security vulnerabilities of Siemens **Simatic S7-300** Firmware : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full ...

CVE-2016-9159 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2016-9159/
Jan 24, 2018 ... A vulnerability has been identified in **SIMATIC S7-300** CPU family, SIMATIC S7- 400 V6 and earlier CPU family, SIMATIC S7-400 V7 CPU family ...

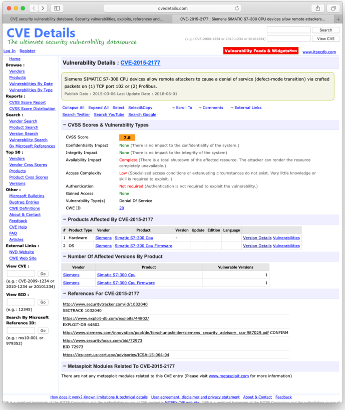
CVE-2015-2177 : Siemens **SIMATIC S7-300** CPU devices allow ...
https://www.cvedetails.com/cve/CVE-2015-2177/
Jun 1, 2018 ... Siemens **SIMATIC S7-300** CPU devices allow remote attackers to cause a denial of service (defect-mode transition) via crafted packets on (1) ...

CVE-2018-16561 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2018-16561/
Apr 19, 2019 ... A vulnerability has been identified in **SIMATIC S7-300** CPUs (All versions < V3.X. 16). The affected CPUs improperly validate S7 communication ...

CVE-2016-9158 : A vulnerability has been identified in **SIMATIC S7** ...
https://www.cvedetails.com/cve/CVE-2016-9158/
Jan 24, 2018 ... A vulnerability has been identified in **SIMATIC S7-300** CPU family, SIMATIC S7- 400 V6 and earlier CPU family, SIMATIC S7-400 V7 CPU family ...

CVE-2016-3949 : Siemens **SIMATIC S7-300** Profinet-enabled CPU ...
https://www.cvedetails.com/cve/CVE-2016-3949/
Aug 18, 2016 ... Siemens **SIMATIC S7-300** Profinet-enabled CPU devices with firmware before 3.2.12 and **SIMATIC S7-300** Profinet-disabled CPU devices with ...

CVE-2016-8672 : The integrated web server on **Siemens SIMATIC** ...
https://www.cvedetails.com/cve/CVE-2016-8672/



Vulnerability Details : CVE-2015-2177

Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of service (defect-mode transition) via crafted packets on (1) TCP port 102 or (2) Profibus.

Publish Date : 2015-03-06 Last Update Date : 2018-06-01

− CVSS Scores & Vulnerability Types

CVSS Score	7.8
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	20

− Products Affected By CVE-2015-2177

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Hardware	Siemens	Simatic S7-300 Cpu	-				Version Details Vulnerabilities
2	OS	Siemens	Simatic S7-300 Cpu Firmware					Version Details Vulnerabilities

− Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Siemens	Simatic S7-300 Cpu	1
Siemens	Simatic S7-300 Cpu Firmware	1

− References For CVE-2015-2177

http://www.securitytracker.com/id/1032040
SECTRACK 1032040

https://www.exploit-db.com/exploits/44802/
EXPLOIT-DB 44802

http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-987029.pdf CONFIRM

http://www.securityfocus.com/bid/72973
BID 72973

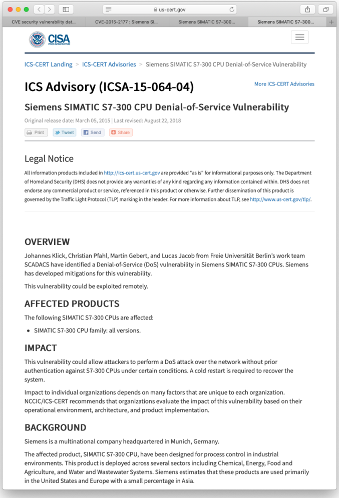
https://ics-cert.us-cert.gov/advisories/ICSA-15-064-04

− Metasploit Modules Related To CVE-2015-2177

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

A denial of service vulnerability

(at least for this version v.0.5/v.2.0.12)


us-cert.gov
CVE security vulnerability dat...
CVE-2015-2177 : Siemens SI...
Siemens SIMATIC S7-300...
Siemens SIMATIC S7-300...
CISA
Print
Tweet
Send
Share

ICS-CERT Landing > ICS-CERT Advisories > Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability

ICS Advisory (ICSA-15-064-04)

More ICS-CERT Advisories

Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability

Original release date: March 05, 2015 | Last revised: August 22, 2018

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Johannes Klick, Christian Pfahl, Martin Gebert, and Lucas Jacob from Freie Universität Berlin's work team SCADACS have identified a Denial-of-Service (DoS) vulnerability in Siemens SIMATIC S7-300 CPUs. Siemens has developed mitigations for this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following SIMATIC S7-300 CPUs are affected:

- SIMATIC S7-300 CPU family: all versions.

IMPACT

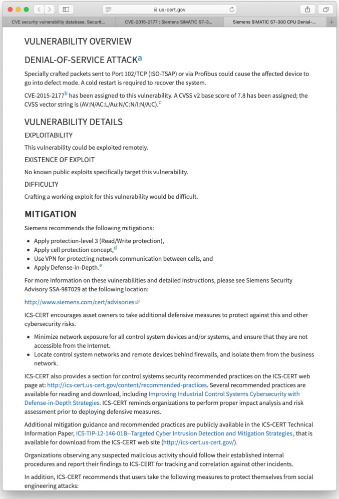
This vulnerability could allow attackers to perform a DoS attack over the network without prior authentication against S7-300 CPUs under certain conditions. A cold restart is required to recover the system.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Siemens is a multinational company headquartered in Munich, Germany.

The affected product, SIMATIC S7-300 CPU, have been designed for process control in industrial environments. This product is deployed across several sectors including Chemical, Energy, Food and Agriculture, and Water and Wastewater Systems. Siemens estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.


us-cert.gov
CVE security vulnerability database. Securit...
CVE-2015-2177 : Siemens SIMATIC S7-3...
Siemens SIMATIC S7-300 CPU Denial-...

VULNERABILITY OVERVIEW

DENIAL-OF-SERVICE ATTACK[a]

Specially crafted packets sent to Port 102/TCP (ISO-TSAP) or via Profibus could cause the affected device to go into defect mode. A cold restart is required to recover the system.

CVE-2015-2177[b] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult.

MITIGATION

Siemens recommends the following mitigations:

- Apply protection-level 3 (Read/Write protection),
- Apply cell protection concept,[d]
- Use VPN for protecting network communication between cells, and
- Apply Defense-in-Depth.[e]

For more information on these vulnerabilities and detailed instructions, please see Siemens Security Advisory SSA-987029 at the following location:

http://www.siemens.com/cert/advisories

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

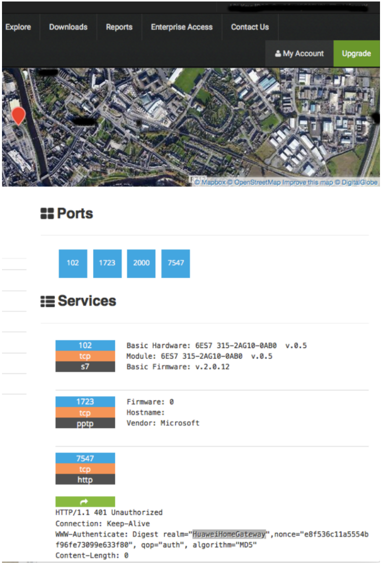
In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;

Preset userid/password `Basisk`;



```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

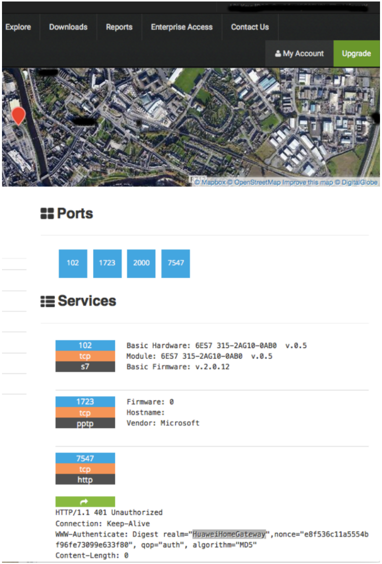
Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;
Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .



```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Vulnerabilities

S7comm on Port 102

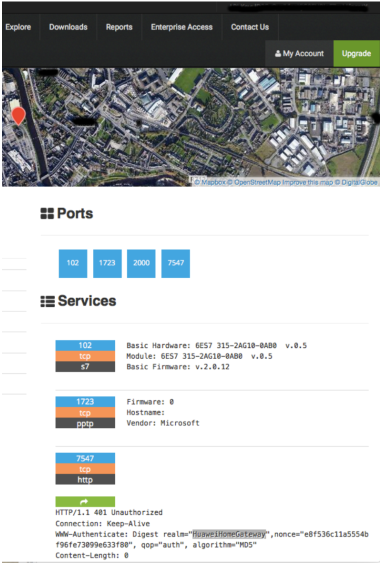
CVE-2015-2177 Denial of service; Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314: MS-CHAPv2 weakness;. . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223: misfortune cookie vulnerability;. . .



[redacted]

[redacted]

[redacted]

Ports

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service; Preset userid/password `Basisk`;

PPTP on Port 1723

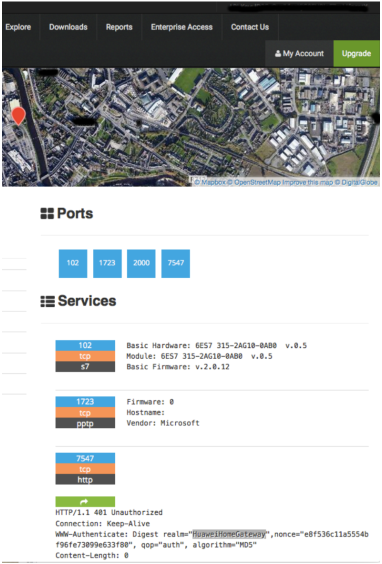
MS Security Advisory 2743314: MS-CHAPv2 weakness;. . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223: misfortune cookie vulnerability;. . .

Huawei home gateway

CVE-2015-7254 path traversal; CVE-2013-6786 embedded web server XSS; . . .



[redacted]

[redacted]

[redacted]

Ports

102 1723 2000 7547

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service; Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314: MS-CHAPv2 weakness;. . .

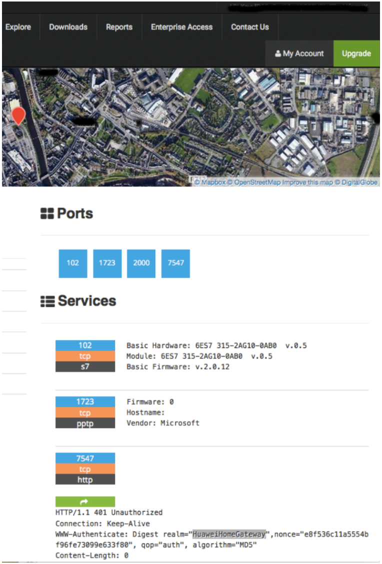
CWMP over HTTP

CVE-2014-9222, CVE-2014-9223: misfortune cookie vulnerability;. . .

Huawei home gateway

CVE-2015-7254 path traversal; CVE-2013-6786 embedded web server XSS; . . .

At least there's no SCADA embedded webserver!



```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

What exactly are the objectives?

The security expert's view

- Security properties, ...
- Setup a VPN, use a firewall, punch a hole for VPN traffic, ..

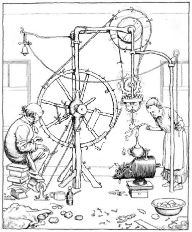
What exactly are the objectives?

The security expert's view

- Security properties, ...
- Setup a VPN, use a firewall, punch a hole for VPN traffic, ..

Convoluted Systems: the user's view

- Configuration efficacy based on user expertise and best practices.
- Dealing with multiple objectives is difficult.



The Professor's invention for peeling potatoes.

Outline of Talk

Networking recap

Motivation

The cautionary tale

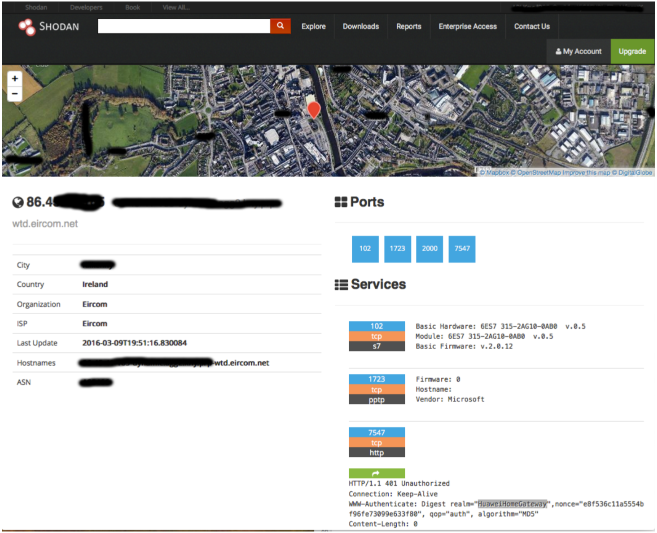
Threat Management

Conclusion

Extra

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102



86.4[redacted] [redacted]

wtd.eircom.net

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-03-09T19:51:16.830084
Hostnames	[redacted]-wtd.eircom.net
ASN	[redacted]

Ports

102 1723 2000 7547

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

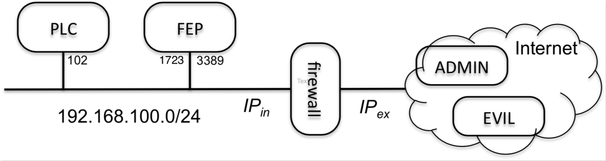
1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554b
f96fe73099e633f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Possible setup behind the scenes?



Use a Virtual Private Network

Virtual Private Network (VPN) is a virtual network established based on the existing public network. VPN uses security techniques such as encryption and identity authentication to ensure confidentiality and security of communication data. For example, to access the company network from your computer, you can connect your computer to the company's VPN server. By doing this, you can securely and easily access network resources on the company network.

Tunnel

What's this?

IP tunnel status: Disconnected

Enable tunnel: □

Siemens FAQ8970169

"Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route"

Original firewall policy

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
2	...	*.*.*.*	$\geq$ 1024	FEP	1723	ALLOW

From: Simon Foley
Subject: XXX Cyber Physical System
Date: March 23, 2016 at 12:02:31 PM GMT+1
To: XXX

Dear XXX,

[...] In preparing a talk on Cyber Physical Systems security I came across an issue on a system which, if I was to guess, is operated by XXX, and wanted to draw your attention to this, in your capacity as [...]

A screenshot with the details is attached and Shodan reports the address of the building as XXX, which, looking at Google Streetview, seems to have some relationship with XXX. In case you're not familiar with it, Shodan.io is an Internet search engine that [...]

Of concern is that Port 102 on the system is reported as open to the Internet. Siemen's S7comm protocol runs over Port 102 and is used for communications between programmable logic controllers and SCADA systems. Looking at the header information it looks like there's a Siemens SIMATIC S7-300 PLC (315-2DP CPU) controller at this address. For example, CVE-2015-2177 [1] notes that versions of the SIMATIC S7-300 is vulnerable to denial of service attack via this protocol as described by Beresford [2], who also discovered a hardcoded userid/password ('Basisk') for internal diagnostic functions [3].

I'm speculating here about the connected system, based on the Shodan report, and no attempt was made to access/test the system.

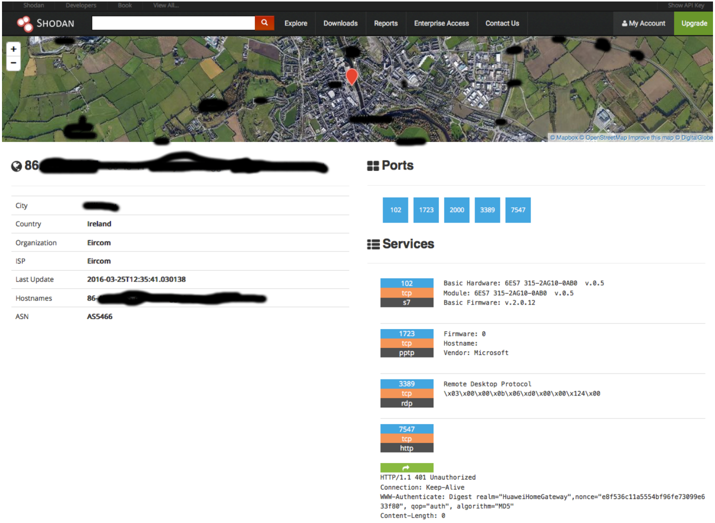
Best practices, for example [4], recommend that the controller and PLCs should be deployed on an internal control network and a VPN tunnel used when accessing the controller over the Internet/public network. VPN access to the local Control Network does appear to be provided via PPTP on Port 1723 on the system, however, it looks like the S7comm Port (102) has been (perhaps accidentally) left open. The S7comm service on Port 102 should not be directly accessible over a public network.

If this is not a XXX controlled system then perhaps you might be able to suggest who the owner might be so that I can contact them?

Best regards,

Simon Foley

Postscript - March 2016



86[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-03-25T12:35:41.030138
Hostnames	86-[redacted]
ASN	AS5466

Ports

102 1723 2000 3389 7547

Services

102 tcp s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

1723 tcp pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

3389 tcp rdp

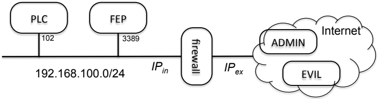
```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

7547 tcp http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554bf96fe73099e6
33f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Firewall policy objectives

(Keep things simple: VPN via Port 3389)

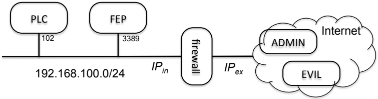


Initial policy *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	ALLOW

Firewall policy objectives

(Keep things simple: VPN via Port 3389)



Initial policy *UPol*

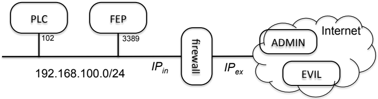
Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	Allow
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	Allow

CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	$\geq$ 1024	PLC	102	Allow
2	...	external IPs	*	PLC	102	Drop
3	...	external IPs	$\geq$ 1024	FEP	3389	Allow

Firewall policy objectives

(Keep things simple: VPN via Port 3389)



Initial policy *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	Allow
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	Allow

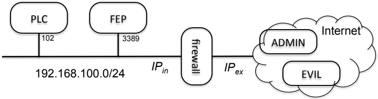
CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	$\geq$ 1024	PLC	102	Allow
2	...	external IPs	*	PLC	102	Drop
3	...	external IPs	$\geq$ 1024	FEP	3389	Allow

Remote Desktop Policy: *RPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	Admin	$\geq$ 1024	FEP	3389	Allow
2	...	*.*.*.*	*	FEP	3389	Drop

Composition of policy objectives

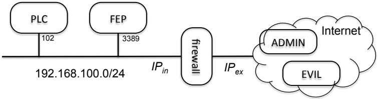


$UPol\,;CPNI\,;RPol$

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	Allow
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	Allow
3	...	192.168.100.0/24	$\geq$ 1024	PLC	102	Allow
4	...	external IPs	*	PLC	102	Drop
5	...	external	$\geq$ 1024	FEP	3389	Allow
6	...	ADMIN	$\geq$ 1024	FEP	3389	Allow
7	...	*.*.*.*	*	FEP	3389	Drop

Each firewall rule takes the form of a series of conditions on packet fields that must be met in order for that rule to be applicable, with a consequent action for the matching packet. Given a network packet, the rules are tested in the order in which they appear in the table. Once a packet has been successfully matched against a rule, no further rule tests are carried out for that packet.

Composition of policy objectives



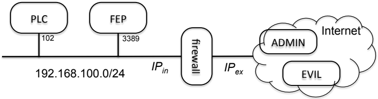
$UPol\,;CPNI\,;RPol$

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	Allow
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	Allow
3	...	192.168.100.0/24	$\geq$ 1024	PLC	102	Allow
4	...	external IPs	*	PLC	102	Drop
5	...	external	$\geq$ 1024	FEP	3389	Allow
6	...	ADMIN	$\geq$ 1024	FEP	3389	Allow
7	...	*.*.*.*	*	FEP	3389	Drop

Each firewall rule takes the form of a series of conditions on packet fields that must be met in order for that rule to be applicable, with a consequent action for the matching packet. Given a network packet, the rules are tested in the order in which they appear in the table. Once a packet has been successfully matched against a rule, no further rule tests are carried out for that packet.

Composition of policy objectives

$\mathit{UPol}\,;\mathit{CPNI}\,;\mathit{RPol}$

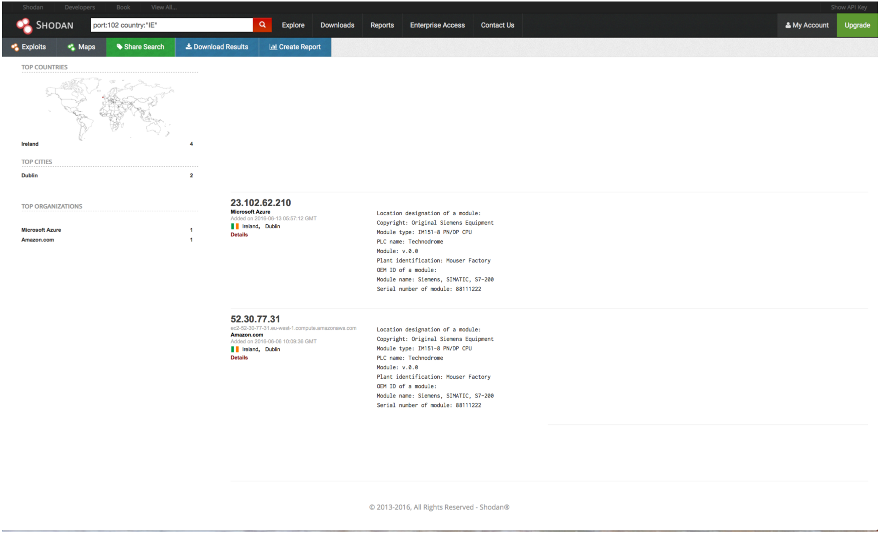


Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	Allow
2	...	*.*.*.*	≥ 1024	FEP	3389	Allow
3	...	192.168.100.0/24	≥ 1024	PLC	102	Allow
4	...	external IPs	*	PLC	102	Drop
5	...	external	≥ 1024	FEP	3389	Allow
6	...	ADMIN	≥ 1024	FEP	3389	Allow
7	...	*.*.*.*	*	FEP	3389	Drop

A *redundancy* conflict occurs when two firewall rules can filter the same packets and those rules have the same target actions over those packets and that the removal of the redundant rule does not affect the semantics of the firewall configuration.

A *shadowing* conflict occurs when a rule is never matched due to a previous rule filtering the same kinds of packets (equivalence or subsumption) and both rules have different target actions.

Postscript - May 2016



TOP COUNTRIES

Ireland	4

TOP CITIES

Dublin	2

TOP ORGANIZATIONS

Microsoft Azure	1
Amazon.com	1

23.102.62.210
Microsoft Azure
Added on 2016-06-13 05:57:12 GMT
Ireland, Dublin
Details

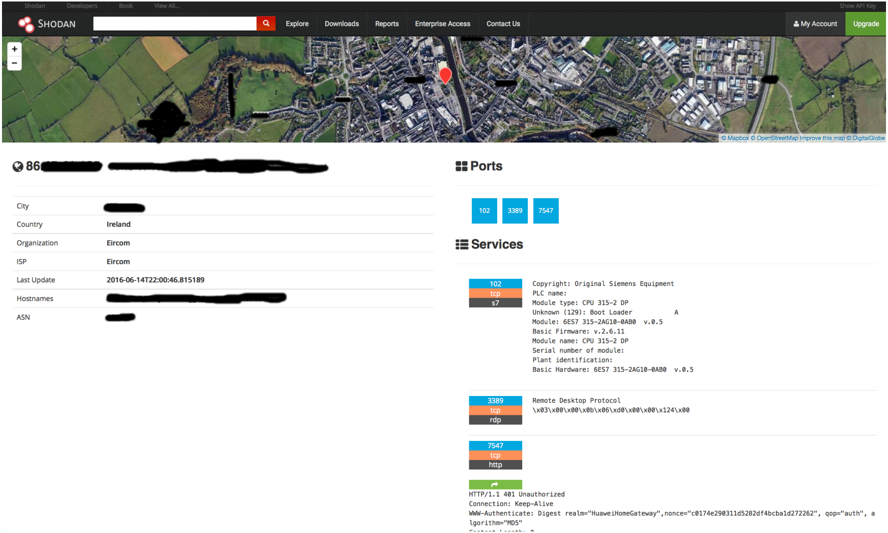
```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

52.30.77.31
ec2-52-30-77-31.eu-west-1.compute.amazonaws.com
Amazon.com
Added on 2016-06-06 10:09:36 GMT
Ireland, Dublin
Details

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

© 2013-2016, All Rights Reserved - Shodan®

Postscript - June 2016



86[redacted] [redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-06-14T22:00:46.815189
Hostnames	[redacted]
ASN	[redacted]

Ports

102 3389 7547

Services

102
tcp
s7

```
Copyright: Original Siemens Equipment
PLC name:
Module type: CPU 315-2 DP
Unknown (129): Boot Loader          A
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.6.11
Module name: CPU 315-2 DP
Serial number of module:
Plant identification:
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
```

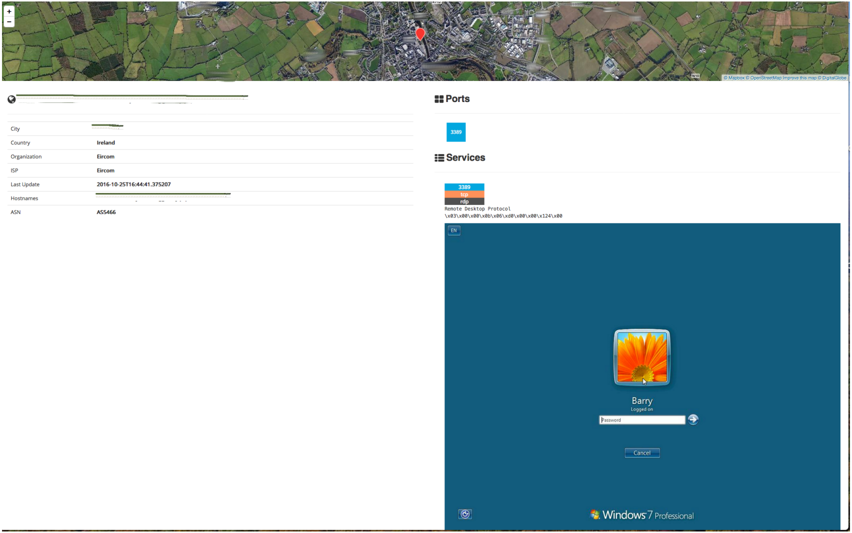
3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

7547
tcp
http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="c0174e290311d5282df4bcba1d272262", qop="auth", a
lgorithm="MD5"
Content-Length: 0
```

Postscript - October 2016



© Mapbox © OpenStreetMap Improve this map © DigitalGlobe

[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-10-25T16:44:41.375207
Hostnames	[redacted]
ASN	AS5466

Ports

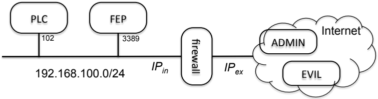
3389

Services

3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

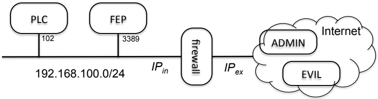
Composition of policy objectives



CPNI ; *RPol* ; *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	$\geq$ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	$\geq$ 1024	FEP	3389	ALLOW
4	...	ADMIN	$\geq$ 1024	FEP	3389	ALLOW
5	...	*.*.*.*	*	FEP	3389	DROP
6	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
7	...	*.*.*.*	$\geq$ 1024	FEP	3389	ALLOW

Composition of policy objectives

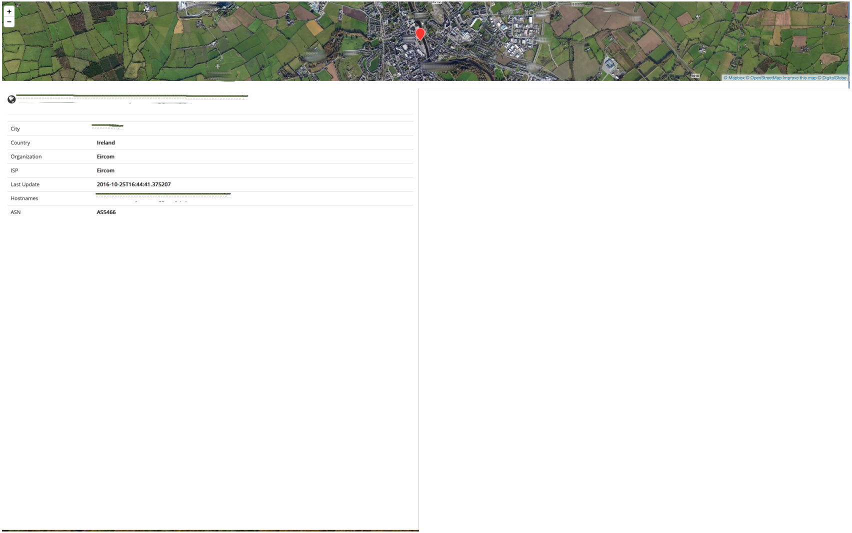


$CPNI\,;RPol\,;UPol$

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	$\geq$ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	$\geq$ 1024	FEP	3389	ALLOW
4	...	ADMIN	$\geq$ 1024	FEP	3389	ALLOW
5	...	*.*.*.*	*	FEP	3389	DROP
6	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
7	...	*.*.*.*	$\geq$ 1024	FEP	3389	ALLOW

[Aside: *redundant* rules can promote policy update inconsistencies: revising one rule may not give the desired effect if there are other redundant rules, or changes become time-consuming as all applicable rules much be searched for and updated.]

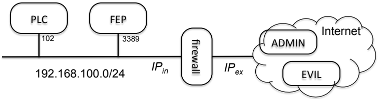
Postscript - December 2016



[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-10-25T16:44:41.375207
Hostnames	[redacted]
ASN	AS5466

Composition of policy objectives



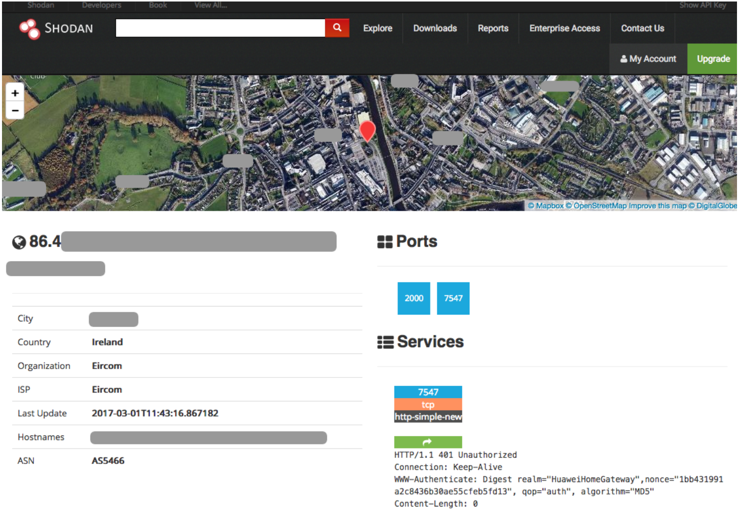
$RPol \, ; CPNI \, ; UPol$

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	ADMIN	$\geq$ 1024	FEP	3389	ALLOW
2	...	*.*.*.*	*	FEP	3389	DROP
3	...	192.168.100.0/24	$\geq$ 1024	PLC	102	ALLOW
4	...	external IPs	*	PLC	102	DROP
5	...	external IPs	$\geq$ 1024	FEP	3389	ALLOW
6	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
7	...	*.*.*.*	$\geq$ 1024	FEP	3389	ALLOW

Wasn't $(RPol; CPNI; UPol)$ obvious?

```
iptables -P FORWARD DROP
iptables -I 1 FORWARD -o eth0 -p icmp –icmp-type echo-request -j DROP
iptables -I 4 FORWARD -o eth0 -s 10.0.0.0/8 -j DROP
iptables -I 11 FORWARD -d PLC --dport 102 -j ACCEPT
iptables -I 1 OUTPUT -p icmp –icmp-type echo-request -j DROP
iptables -I 5 FORWARD -o eth0 -s 172.16.0.0/12 -j DROP
iptables -I 6 FORWARD -i eth0 -s 192.168.0.0/16 -j DROP
iptables -I 7 FORWARD -o eth0 -s 224.0.0.0/4 -j DROP
iptables -I 8 FORWARD -o eth0 -s 240.0.0.0/5 -j DROP
iptables -I 9 FORWARD -o eth0 -s 127.0.0.0/8 -j DROP
iptables -I 10 FORWARD -o eth0-s 0.0.0.0/8 -j DROP
iptables -I 11 FORWARD -d FEP --dport 3398 -j ACCEPT
iptables -I 12 FORWARD -o eth0 -d 255.255.255.255 -j DROP
iptables -I 13 FORWARD -o eth0 -s 169.254.0.0/16 -j DROP
iptables -I 14 FORWARD -o eth0 -d 224.0.0.0/4 -j DROP
iptables -I 15 FORWARD -p tcp –tcp-flags ACK,URG URG -j DROP
iptables -I 16 FORWARD -p tcp –tcp-flags FIN,RST FIN,RST -j DROP
iptables -I 17 FORWARD -p tcp –tcp-flags SYN,FIN SYN,FIN -j DROP
iptables -I 19 FORWARD -p tcp –tcp-flags SYN,RST SYN,RST -j DROP
iptables -I 11 FORWARD -d PLC --dport 102 -j DROP
iptables -I 20 FORWARD -p tcp –tcp-flags ALL ALL -j DROP
iptables -I 21 FORWARD -p tcp –tcp-flags ALL NONE -j DROP
iptables -I 22 FORWARD -p tcp –tcp-flags ALL FIN,PSH,URG -j DROP
iptables -I 23 FORWARD -p tcp –tcp-flags ALL SYN,FIN,PSH,URG -j DROP
....
...
```

Postscript - 03 March 2017



86.4[redacted]

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-01T11:43:16.867182**
Hostnames	[redacted]
ASN	**AS5466**

Ports

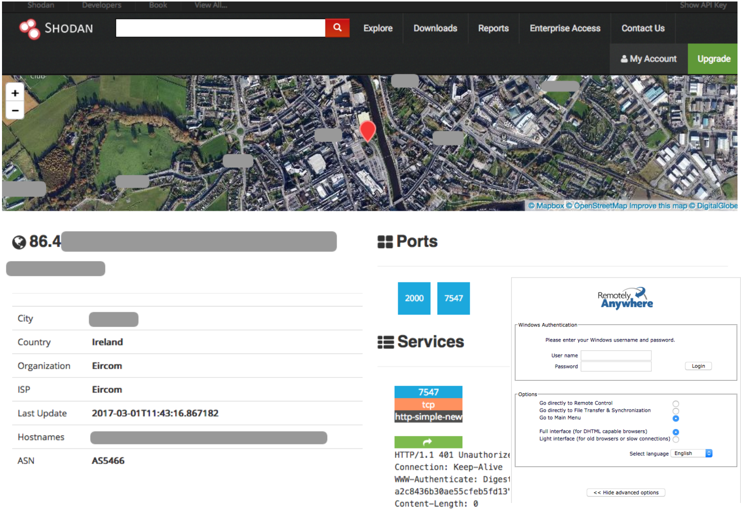
2000 7547

Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="1bb431991
a2c8436b30ae55cfeb5fd13", qop="auth", algorithm="MD5"
Content-Length: 0
```

Postscript - 03 March 2017



86.4[redacted]

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-01T11:43:16.867182**
Hostnames	[redacted]
ASN	**AS5466**

Ports

2000 7547

Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorize
Connection: Keep-Alive
WWW-Authenticate: Digest
a2c8436b30ae55cfeb5fd13'
Content-Length: 0
```

Windows Authentication

Please enter your Windows username and password.

User name
Password
Login

Options

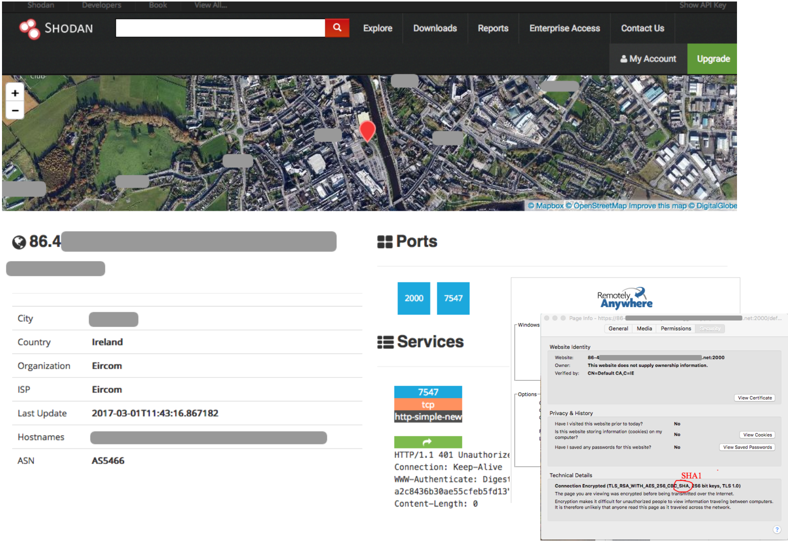
Go directly to Remote Control ○
Go directly to File Transfer & Synchronization ○
Go to Main Menu ●

Full interface (for DHTML capable browsers) ●
Light interface (for old browsers or slow connections) ○

Select language English

<< Hide advanced options

Postscript - 03 March 2017



86.4[redacted]

[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2017-03-01T11:43:16.867182
Hostnames	[redacted]
ASN	AS5466

Ports

2000 7547

Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorize
Connection: Keep-Alive
WWW-Authenticate: Digest
a2c8436b30ae55cfeb5fd13'
Content-Length: 0
```

Page Info - https://86-[redacted].net:2000/def...

General Media Permissions Security

Website Identity

Website: 86-4[redacted].net:2000
Owner: This website does not supply ownership information.
Verified by: CN=Default CA,C=IE

View Certificate

Privacy & History

Have I visited this website prior to today?	No	
Is this website storing information (cookies) on my computer?	No	View Cookies
Have I saved any passwords for this website?	No	View Saved Passwords

Technical Details

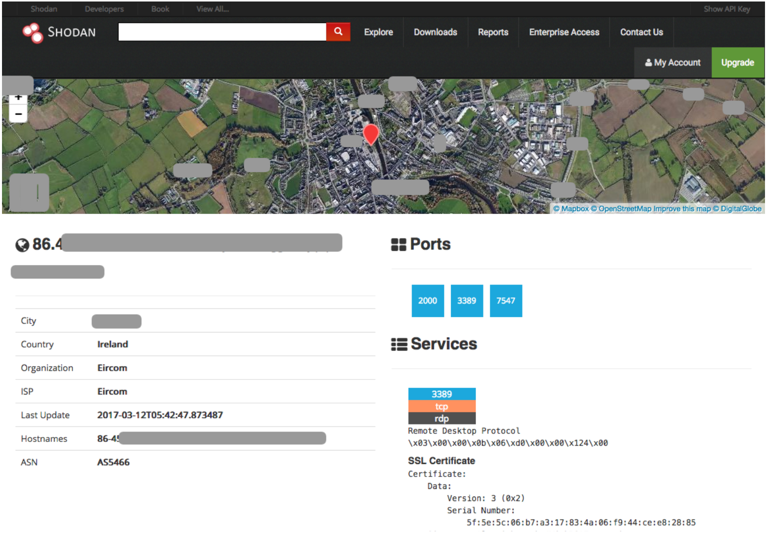
SHA1

Connection Encrypted (TLS_RSA_WITH_AES_256_CBC_SHA, 256 bit keys, TLS 1.0)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Postscript - 13 March 2017



86.4[redacted]

[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2017-03-12T05:42:47.873487
Hostnames	86-4[redacted]
ASN	AS5466

Ports

2000 3389 7547

Services

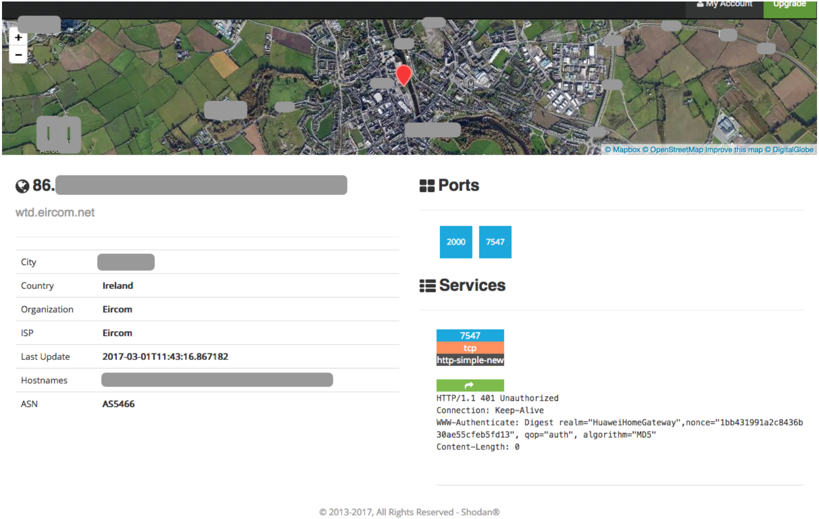
3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5f:5e:5c:06:b7:a3:17:83:4a:06:f9:44:ce:e8:28:85
```

Postscript - 17 March 2017



86.[redacted]

wtd.eircom.net

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2017-03-01T11:43:16.867182
Hostnames	[redacted]
ASN	AS5466

Ports

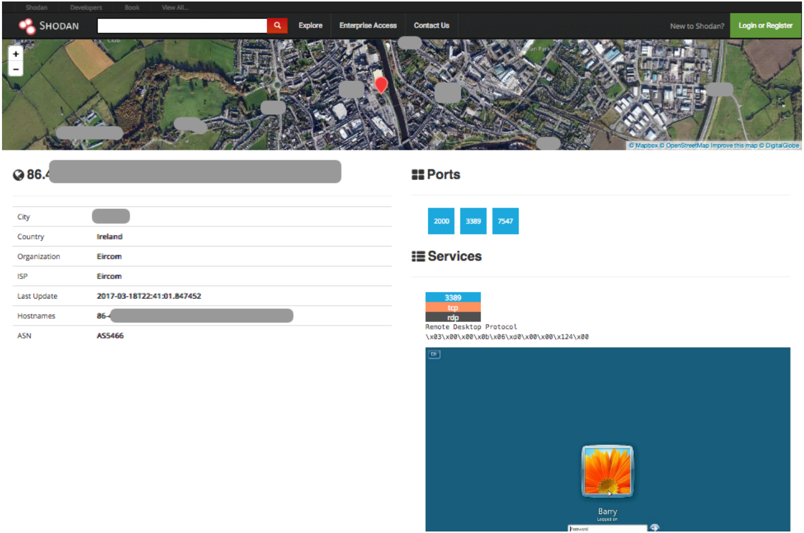
2000 7547

Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="1bb431991a2c8436b
30ae55cfeb5fd13", qop="auth", algorithm="MD5"
Content-Length: 0
```

Postscript - 20 March 2017



86.[redacted]

City	[redacted]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2017-03-18T22:41:01.847452
Hostnames	86-[redacted]
ASN	AS5466

Ports: 2000 3389 7547

3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

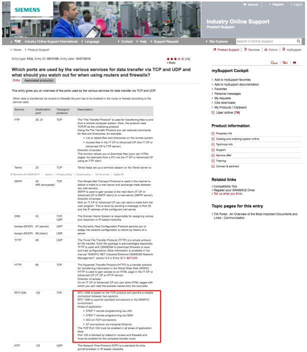
Extra

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open



Entry type: FAQ, Entry ID: 8970169, Entry date: 10/27/2016

Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routers and firewalls?

This entry gives you an overview of the ports used by the various services for data transfer via TCP and UDP.

When data is transferred via routers or firewalls the port has to be enabled in the router or firewall according to the service used.

Service	Destination port	Transport protocol	Description
FTP	20, 21	TCP	The "File Transfer Protocol" is used for transferring files to and from a remote computer system. Here, the protocol uses TCP/IP as the underlying protocol. Using the File Transfer Protocol you can execute commands for files and directories, for example: • List or delete files and directories on the remote system • Access files in the IT CP or Advanced CP (the IT CP or Advanced CP is FTP server). Direction of access This function allows you to download files (your own HTML pages, for example) from a PC into the IT CP or Advanced CP using an FTP client.
Telnet	23	TCP	Telnet helps set up a terminal session on the Telnet server to
SMTP	25 465 (encrypted)	TCP	The Simple Mail Transport Protocol is used in the internet to deliver e-mails to a mail server and exchange mails between two mail servers. SMTP is used to gain access to the mail client (IT CP or Advanced CP is SMTP client) on a mail server (SMTP server). Direction of access With an IT CP or Advanced CP you can send e-mails from the user program. This is done by sending a message to Port 25 and the IP address of the configured mail server.
DNS	53	TCP, UDP	The Domain Name System is responsible for assigning names and resolution in IP-based networks.
bootps (DHCP)	67 (server)	UDP	The Dynamic Host Configuration Protocol permits you to assign the network configuration to clients by means of a server.
bootpc (DHCP)	68 (client)	UDP	
TFTP	69	UDP	The Trivial File Transfer Protocol (TFTP) is a simple protocol for file transfer. Each file package is acknowledged separately. TFTP is used with OSM/ESM to download firmware or save and load configurations. More information is available in the manual "SIMATIC NET Industrial Ethernet OSM/ESM Network Management", section 6.3 in Entry ID > 8677203.
HTTP	80	TCP	The Hypertext Transfer Protocol (HTTP) is a transfer protocol for transferring information in the World Wide Web (WWW). HTTP is used to gain access to an HTML page in the IT CP or Advanced CP (IT CP is HTTP server). Direction of access On an IT CP or Advanced CP you can store HTML pages with which you can read the process values from the controller.
RFC1006	102	TCP	RFC 1006 is based on the TCP protocol and permits a reliable connection between two systems. RFC 1006 is used for standard connections in the SIMATIC environment. Areas of application: • STEP 7 remote programming via LAN • STEP 7 remote programming via ISDN • ISO-on-TCP connections • S7 connections via Industrial Ethernet The TCP Port 102 must be enabled in all areas of application. Note Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route.
NTP	123	UDP	The Network Time Protocol (NTP) is a standard for time synchronization in IP-based networks.

© Siemens AG 2009-2017 - Imprint | Privacy policy | Cookie policy | Terms of use | Digital ID

mySupport Cockpit

- Add to mySupport favorites
- Add to mySupport documentation
- Favorites
- Personal messages
- My requests
- CAx downloads
- My Products / Clipboard
- User online (74)

Product information

- Presales info
- Catalog and ordering system online
- Technical info
- Support
- Service offer
- Training
- Contact & partners

Related links

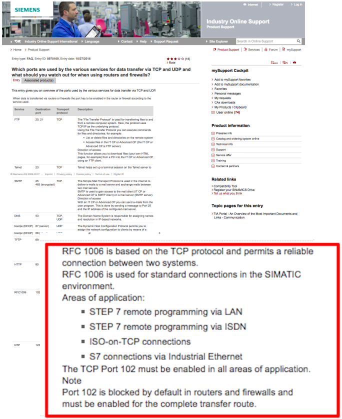
- Compatibility Tool
- Register your SINAMICS Drive
- Tell us what you think

Topic pages for this entry

- TIA Portal - An Overview of the Most Important Documents and Links - Communication

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open



Entry type: FAQ, Entry ID: 8970169, Entry date: 10/27/2016

★★★☆☆ (15)

Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routers and firewalls?

This entry gives you an overview of the ports used by the various services for data transfer via TCP and UDP.

When data is transferred via routers or firewalls the port has to be enabled in the router or firewall according to the service used.

Service	Destination port	Transport protocol	Description
FTP	20, 21	TCP	The "File Transfer Protocol" is used for transfering files to and from a remote computer system. Here, the protocol uses TCP/IP as the underlying protocol. Using the File Transfer Protocol you can execute commands for files and directories, for example: • List or delete files and directories on the remote system • Access files in the IT CP or Advanced CP (the IT CP or Advanced CP is FTP server). Direction of access This function allows you to download files (your own HTML pages, for example) from a PC into the IT CP or Advanced CP using an FTP client.
Telnet	23	TCP	Telnet helps set up a terminal session on the Telnet server to
SMTP	25 465 (encrypted)	TCP	The Simple Mail Transport Protocol is used in the internet to deliver e-mails to a mail server and exchange mails between two mail servers. SMTP is used to gain access to the mail client (IT CP or Advanced CP is SMTP client) on a mail server (SMTP server). Direction of access With an IT CP or Advanced CP you can send e-mails from the user program. This is done by sending a message to Port 25 and the IP address of the configured mail server.
DNS	53	TCP, UDP	The Domain Name System is responsible for assigning names and resolution in IP-based networks.
bootps (DHCP)	67 (server)	UDP	The Dynamic Host Configuration Protocol permits you to assign the network configuration to clients by means of a
bootpc (DHCP)	68 (		
TFTP	69		
HTTP	80		
RFC1006	102		
NTP	123		

© Siemens AG 2009-2017 - Imprint | Privacy policy | Cookie policy | Terms of use | Digital ID

mySupport Cockpit

- Add to mySupport favorites
- Add to mySupport documentation
- Favorites
- Personal messages
- My requests
- CAx downloads
- My Products / Clipboard
- User online (74)

Product information

- Presales info
- Catalog and ordering system online
- Technical info
- Support
- Service offer
- Training
- Contact & partners

Related links

- Compatibility Tool
- Register your SINAMICS Drive
- Tell us what you think

Topic pages for this entry

- TIA Portal - An Overview of the Most Important Documents and Links - Communication

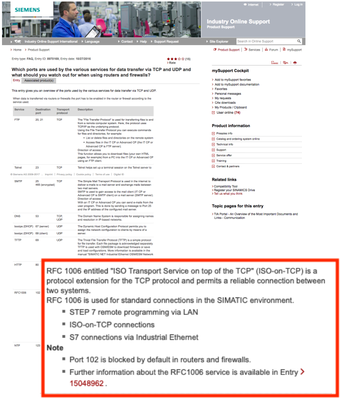
RFC 1006 is based on the TCP protocol and permits a reliable connection between two systems.
RFC 1006 is used for standard connections in the SIMATIC environment.
Areas of application:

- STEP 7 remote programming via LAN
- STEP 7 remote programming via ISDN
- ISO-on-TCP connections
- S7 connections via Industrial Ethernet

The TCP Port 102 must be enabled in all areas of application.
Note
Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route.

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ



SIEMENS

Internet | Register | Log in

Industry Online Support
Product Support

Industry Online Support International | Language | Contact | Help | Support Request | Site Explorer | Search in Online Support

Home > Product Support

Product Support | Services | Forum | mySupport

Entry type: FAQ, Entry ID: 8970169, Entry date: 10/27/2016

★★★☆☆ (15)
Rate

Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routers and firewalls?

Entry | Associated product(s)

This entry gives you an overview of the ports used by the various services for data transfer via TCP and UDP.

When data is transferred via routers or firewalls the port has to be enabled in the router or firewall according to the service used.

Service	Destination port	Transport protocol	Description
FTP	20, 21	TCP	The "File Transfer Protocol" is used for transferring files to and from a remote computer system. Here, the protocol uses TCP/IP as the underlying protocol. Using the File Transfer Protocol you can execute commands for files and directories, for example: • List or delete files and directories on the remote system • Access files in the IT CP or Advanced CP (the IT CP or Advanced CP is FTP server). Direction of access This function allows you to download files (your own HTML pages, for example) from a PC into the IT CP or Advanced CP using an FTP client.
Telnet	23	TCP	Telnet helps set up a terminal session on the Telnet server to
SMTP	25 465 (encrypted)	TCP	The Simple Mail Transport Protocol is used in the internet to deliver e-mails to a mail server and exchange mails between two mail servers. SMTP is used to gain access to the mail client (IT CP or Advanced CP is SMTP client) on a mail server (SMTP server). Direction of access With an IT CP or Advanced CP you can send e-mails from the user program. This is done by sending a message to Port 25 and the IP address of the configured mail server.
DNS	53	TCP, UDP	The Domain Name System is responsible for assigning names and resolution in IP-based networks.
bootps (DHCP)	67 (server)	UDP	The Dynamic Host Configuration Protocol permits you to assign the network configuration to clients by means of a server.
bootpc (DHCP)	68 (client)	UDP	
TFTP	69	UDP	The Trivial File Transfer Protocol (TFTP) is a simple protocol for file transfer. Each file package is acknowledged separately. TFTP is used with OSM/ESM to download firmware or save and load configurations. More information is available in the manual "SIMATIC NET Industrial Ethernet OSM/ESM Network
HTTP	80		
RFC1006	102		
NTP	123		

© Siemens AG 2009-2017 - Imprint | Privacy policy | Cookie policy | Terms of use | Digital ID

mySupport Cockpit

- Add to mySupport favorites
- Add to mySupport documentation
- Favorites
- Personal messages
- My requests
- CAx downloads
- My Products / Clipboard
- User online (74)

Product information

- Presales info
- Catalog and ordering system online
- Technical info
- Support
- Service offer
- Training
- Contact & partners

Related links

- Compatibility Tool
- Register your SINAMICS Drive
- Tell us what you think

Topic pages for this entry

- TIA Portal - An Overview of the Most Important Documents and Links - Communication

RFC 1006 entitled "ISO Transport Service on top of the TCP" (ISO-on-TCP) is a protocol extension for the TCP protocol and permits a reliable connection between two systems.
RFC 1006 is used for standard connections in the SIMATIC environment.

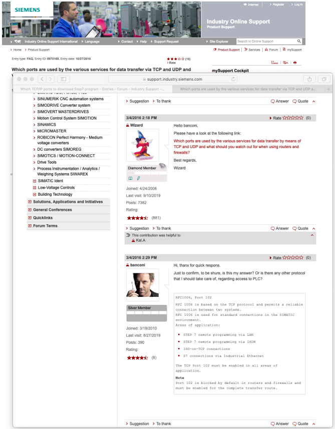
- STEP 7 remote programming via LAN
- ISO-on-TCP connections
- S7 connections via Industrial Ethernet

Note

- Port 102 is blocked by default in routers and firewalls.
- Further information about the RFC1006 service is available in Entry › 15048962 .

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ
- But, we also look for advice elsewhere.


SIEMENS
Internet
Register
Log in
Industry Online Support
Product Support
Industry Online Support International
Language
Contact
Help
Support Request
Site Explorer
Search in Online Support
Home
Product Support
Product Support
Services
Forum
mySupport
Rate
mySupport Cockpit
support.industry.siemens.com
Which TCP/IP ports to download Step7 program - Entries - Forum - Industry Support -...
Which ports are used by the various services for data transfer via TCP and UDP a...
SINUMERIK CNC automation systems
SIMODRIVE Converter system
SIMOVERT MASTERDRIVES
Motion Control System SIMOTION
SINAMICS
MICROMASTER
ROBICON Perfect Harmony - Medium voltage converters
DC converters SIMOREG
SIMOTICS / MOTION-CONNECT
Drive Tools
Process Instrumentation / Analytics / Weighing Systems SIWAREX
SIMATIC Ident
Low-Voltage Controls
Building Technology
Solutions, Applications and Initiatives
General Conferences
Quicklinks
Forum Terms
Suggestion
To thank
Answer
Quote
Diamond Member
Silver Member

Entry type: **FAQ**, Entry ID: **8970169**, Entry date: **10/27/2016** ★★★☆☆ (15)

Which ports are used by the various services for data transfer via TCP and UDP and

3/4/2016 2:18 PM Rate ☆☆☆☆☆ (0)

Wizard

Hello banconi,

Please have a look at the following link:

Which ports are used by the various services for data transfer by means of TCP and UDP and what should you watch out for when using routers and firewalls?

Best regards,

Wizard

Joined: 4/24/2006
Last visit: 9/10/2019
Posts: 7382
Rating:
★★★★☆ (881)

This contribution was helpful to
Kal.A

3/4/2016 2:29 PM Rate ☆☆☆☆☆ (0)

banconi

Hi, thanx for quick respons.

Just to confirm, to be shure, is this my answer? Or is there any other protocol that I should take care of, regarding access to PLC?

```
RFC1006, Port 102

RFC 1006 is based on the TCP protocol and permits a reliable
connection between two systems.
RFC 1006 is used for standard connections in the SIMATIC
environment.
Areas of application:

 ▪ STEP 7 remote programming via LAN
 ▪ STEP 7 remote programming via ISDN
 ▪ ISO-on-TCP connections
 ▪ S7 connections via Industrial Ethernet

The TCP Port 102 must be enabled in all areas of
application.

Note
Port 102 is blocked by default in routers and firewalls and
must be enabled for the complete transfer route.
```

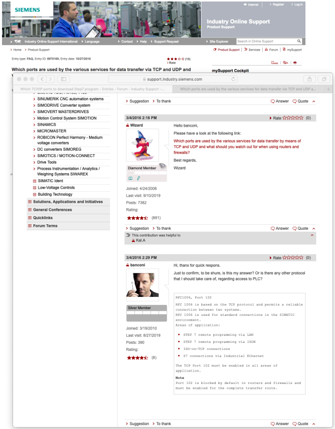
Joined: 3/19/2010
Last visit: 8/27/2019
Posts: 390
Rating:
★★★★☆ (8)

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ
- But, we also look for advice elsewhere.

Following a control recommendation does not necessarily mean threat is mitigated.

Must also check the efficacy of the control at mitigating the threat.


SIEMENS
Internet
Register
Log in
Industry Online Support
Product Support
Industry Online Support International
Language
Contact
Help
Support Request
Site Explorer
Search in Online Support
Home
Product Support
Services
Forum
mySupport
Rate
mySupport Cockpit
support.industry.siemens.com
Which TCP/IP ports to download Step7 program - Entries - Forum - Industry Support -...
Which ports are used by the various services for data transfer via TCP and UDP a...
SINUMERIK CNC automation systems
SIMODRIVE Converter system
SIMOVERT MASTERDRIVES
Motion Control System SIMOTION
SINAMICS
MICROMASTER
ROBICON Perfect Harmony - Medium voltage converters
DC converters SIMOREG
SIMOTICS / MOTION-CONNECT
Drive Tools
Process Instrumentation / Analytics / Weighing Systems SIWAREX
SIMATIC Ident
Low-Voltage Controls
Building Technology
Solutions, Applications and Initiatives
General Conferences
Quicklinks
Forum Terms
Suggestion
To thank
Answer
Quote
Diamond Member
Silver Member

Entry type: FAQ, Entry ID: 8970169, Entry date: 10/27/2016

★★★☆☆ (15)

Which ports are used by the various services for data transfer via TCP and UDP and

3/4/2016 2:18 PM Rate ☆☆☆☆☆ (0)

Wizard

Joined: 4/24/2006
Last visit: 9/10/2019
Posts: 7382
Rating: ★★★★☆ (881)

Hello banconi,

Please have a look at the following link:

Which ports are used by the various services for data transfer by means of TCP and UDP and what should you watch out for when using routers and firewalls?

Best regards,

Wizard

This contribution was helpful to
Kal.A

3/4/2016 2:29 PM Rate ☆☆☆☆☆ (0)

banconi

Joined: 3/19/2010
Last visit: 8/27/2019
Posts: 390
Rating: ★★★★☆ (8)

Hi, thanx for quick respons.

Just to confirm, to be shure, is this my answer? Or is there any other protocol that I should take care of, regarding access to PLC?

```
RFC1006, Port 102
RFC 1006 is based on the TCP protocol and permits a reliable
connection between two systems.
RFC 1006 is used for standard connections in the SIMATIC
environment.
Areas of application:

  • STEP 7 remote programming via LAN
  • STEP 7 remote programming via ISDN
  • ISO-on-TCP connections
  • S7 connections via Industrial Ethernet

The TCP Port 102 must be enabled in all areas of
application.
Note
Port 102 is blocked by default in routers and firewalls and
must be enabled for the complete transfer route.
```

Security threat management for the ICS use case

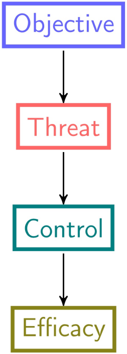
Objective: provide remote supervisory control to ICS

Threat: attacker accesses PLC

- CPNI: tunnel S7 traffic over VPN.
- Only admin IP may access via VPN.
- Software update mechanism.

Efficacy: are threats mitigated?

- Check VPN/firewall is configured.
- Audit HW/SW versions, run shodan, ...
- IDS checks for suspicious S7 packets on internal network.



Security threat management for the ICS use case

Objective: provide remote supervisory control to ICS

Threat: attacker accesses PLC

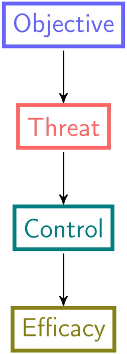
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP may access via VPN.
- Software update mechanism.

Efficacy: are threats mitigated?

- Check VPN/firewall is configured.
- Audit HW/SW versions, run shodan, ...
- IDS checks for suspicious S7 packets on internal network.

Threat: PLC is unreachable

- FAQ: “[...] open Port 102 on router”



Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

Conclusion

- Security control selection does not necessarily mean system is secure: controls can conflict, be ineffective or missing.
- Assess the efficacy of threat mitigation: intrusion detection, ongoing audit, shodan investigation, ...
- Policy anomalies: what is meant by policy composition?
- Vulnerabilities are not limited to code.
- Studies help us to understand *why*.

Resources and further reading

- https://shodan.io
- *"Journalists warned system owners and Norwegian NSA of 2500 critical data flaws"*, Dagbladet, 06.01.2014.
- Dagbladet, NULL CTRL, https://www.dagbladet.no/nullctrl
- Front-end for CVE data https://www.cvedetails.com
- SN Foley, *Getting security objectives wrong: a cautionary tale of an Industrial Control System*, In proceedings of International Workshop on Security Protocols, Springer LNCS 10476, 2017.
- Robert Graham, FAQ: Firewall Forensics (What am I seeing?), Linux Security, 2000.

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

Responsible disclosure

Give stakeholders opportunity to address issues

- Contacted owners of email sites about SMTP vulnerabilities.
- Contacted ICS owner about the Scada/other vulnerabilities.
- Contacted Siemens about the ‘confusion’ in FAQ 8970169.

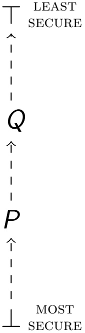
Shodan investigation only; did not visit/probe the sites

Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.

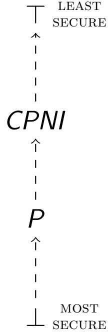


Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.
- Compliance: $P \sqsubseteq CPNI$

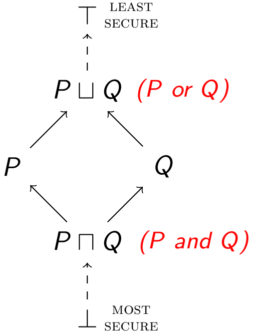


Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q.
- Currently upheld objective Q can be securely replaced by objective P.
- Compliance: $P \sqsubseteq CPNI$



Secure Composition $P \sqcap Q$, $P \sqcup Q$

- A lattice of policy objectives.
- Objective $P \sqcap Q$ as 'best' objective that is no less secure than P and Q.
- Replace P by $P \sqcap (CPNI \sqcup RFC5735)$

A (simplified) lattice of firewall policies

Secure Replacement $P \sqsubseteq Q$

Policy Q can be replaced by policy P, if P is no less restrictive than Q. For all $P, Q : Policy$:

$$\begin{array}{rcl} P \sqsubseteq Q & \equiv & (accepts(P) \subseteq accepts(Q)) \wedge (denies(P) \supseteq denies(Q)) \\ P \sqcup Q & \Leftrightarrow & (accepts(P) \cup accepts(Q)) \wedge (denies(P) \cap denies(Q)) \\ P \sqcap Q & \Leftrightarrow & (accepts(P) \cap accepts(Q)) \wedge (denies(P) \cup denies(Q)) \end{array}$$

Lattice of policies $(Policy, \sqsubseteq, \sqcup, \sqcap)$

A lattice under $\sqsubseteq$; lowest upper bound $\sqcup$ and greatest lower bound $\sqcap$.

Policy compositions

$$\begin{array}{rcl} Pol & = & UPol \sqcap (CPNI \sqcup RPol) \\ & = & (RPol \fatsemi CPNI \fatsemi UPol); \\ Pol' & = & Pol \sqcap RFC5735 \end{array}$$

Some sample Snort IDS rules

We could configure an IDS to look for any traffic that might suggest attempted use of the built-in Basisk Siemens account, for instance a Snort style rule that looks for any packet containing string "Basisk":

```
alert TCP any any -> any 102 \
     (msg:"access attempt using Basisk backdoor account"; \
      content:"Basisk";  )
```

However, this is a coarse-grained rule: we would like to be able to discriminate an attack on a vulnerable system (that could succeed), versus a unsuccessful attempt against a non-vulnerable system (that could not succeed).

It is also possible that access to this hard-coded account on legacy systems via the local network might be considered a necessary operation for certain legacy workflows.

Some Snort IDS rules for Simatic S7 can be found here and here

Some sample Snort IDS rules

Stateful rule attribute `flowbits` is used to track rule state during a transport protocol session. It's set to `backdoor` when it appears that there is a S7 connection attempt made using the backdoor `Basisk` userid/password.

```
alert TCP any any -> any 102 \
    (msg:"access attempt using Basisk backdoor account"; \
     content:"Basisk";  \
     flow:to_server,established; \
     flowbits:set,backdoor; )
```

If there is subsequent activity on the attempted `Basisk` TCP session then it could indicate that the login was successful. The following rule triggers an alert if it appears that there is an attempt to send a request to delete a block over that same session:

```
alert tcp any any -> any 102  \
    (msg:"Delete block requested via backdoor account"; \
     content:"|03 00|";offset:0;depth:2; \
     content:"|05 5f 44 45 4c 45|";sid:20; \
     flow:to_server,established; \
     flowbits:isset,backdoor; )
```

However, the correlation here is crude.