How Many Bugs Can a Time Server Have?

Tim Brown – Head Of Research

Mike Emery – Researcher

Content/Topics

- What this talk will cover
  - What we tested
  - How we tested the device
  - What we found
  - Why it's bad

What Did We Test?

- Symmetricom (Micro Semi) S350i

Who Would Buy One?

- No-one Important
  - Financial Institutions
  - Medical
  - Energy
  - Aviation
  - Communications
  - Defence
  - Security
  - Industrial...

The Attack Surface

- Physical
  - USB
  - Serial
  - Network Ports
  - Buttons
- Logical
  - Management network
  - Production network
  - Authorised

Physical: USB

- Updates
- Configuration backups
- Peripherals

```
/etc/mvl-release:

MontaVista Linux Version 4.0.1, Professional Edition (0600996)
```

Physical: Serial

- Boot time
- Console access

Physical: Network Ports

- Different ports = Different networks = Different services

Physical: Buttons

- Change settings
- Make backups
- PIN

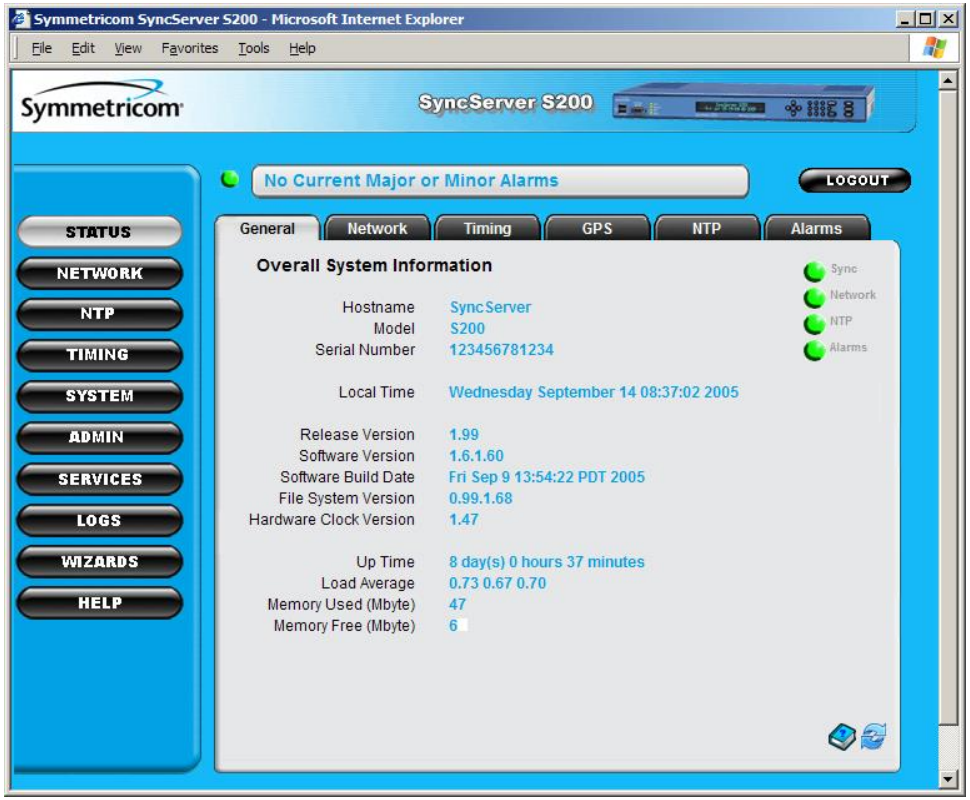
```
/etc/dispd.conf:

# Keypad lockout password
Password=123
```

Logical: Management

- Web interface
- SSH
- SNMP
- PostgreSQL(?!)

Management: Web interface

- Just awful- Blame J. Costanza

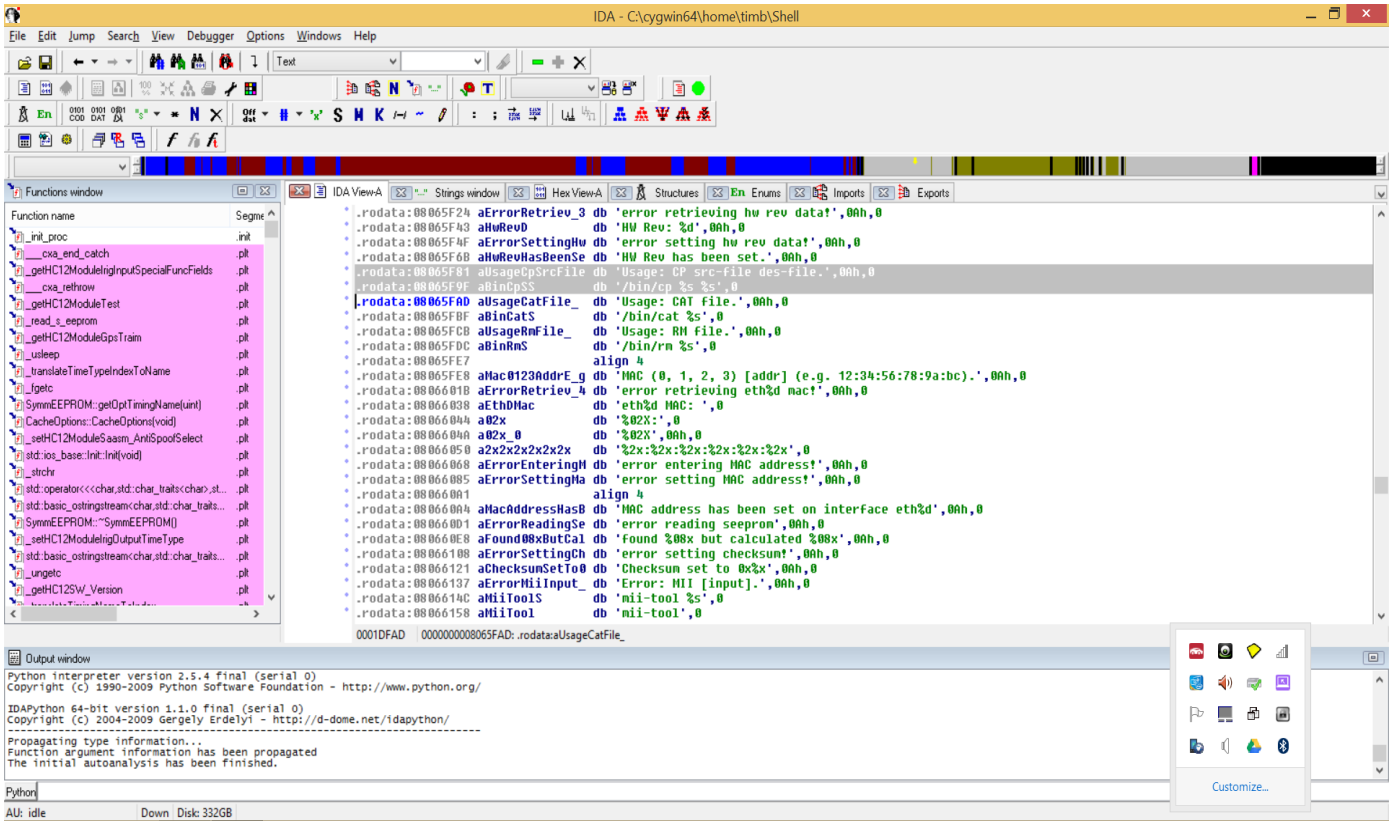


Management: Web interface

- CVE-2014-5071: SQL Injection
- CVE-2014-5070: Vertical Privilege Escalation
- CVE-2014-5069: Stored XSS
- CVE-2014-5068: Directory Traversal
- CVE-2014-5067: Arbitrary File Upload
- But who cares? CVE-2014-5061: Remote Root

Management: SSH

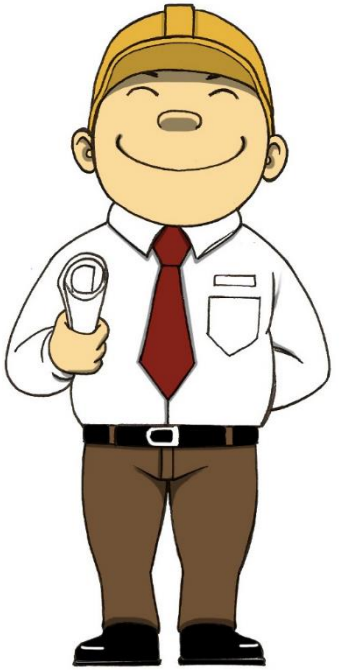
- WTH is this shell?



Management: SSH

- CVE-2014-5062: Shell Breakout

```
<NN> ? root engineering
<NN> ? sys
<NN> ? cp /z /zz;id
<NN> ? cp /z /zz;/bin/bash
...
<NN> ? ifconf lo;id
<NN> ? ping 8.8.8.8;id
```



THE HELPFUL ENGINEER

Management: SNMP

```
UCD-SNMP-MIB::versionConfigureOptions.0 = STRING: '--host=i586-montavista-
linux' '--build=i686-pc-linux-gnu' '--prefix=/usr' '--exec-prefix=/usr' '--
bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--
datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib' '--
libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/share'
'--mandir=/usr/share/man' '--infodir=/usr/share/info' '--
includedir=/usr/include/net-snmp' '--with-persistent-directory=/var/net-snmp'
'--enable-ipv6' '--enable-shared' '--with-libwrap' '--with-logfile=' '--with-
openssl=/home/buildslave/syncserver-buildbot/s3xx-centurion-experimental/s3xx-
centurion-experimental/build' '--without-dmalloc' '--without-efense' '--with-
sys-contact=root@localhost' '--with-sys-location=unknown' '--with-mib-
modules=symmetricom' '--without-rpm' '--with-endianness=little' '--with-perl-
modules' '--with-defaults' 'CC=586-gcc ' 'CFLAGS=-I/home/buildslave/syncserver-
buildbot/s3xx-centurion-experimental/s3xx-centurion-experimental/build/include
-I/home/buildslave/syncserver-buildbot/s3x
```

Management: PostgreSQL

- Used by a Java Applet in the Web Management
- CVE-2014-5064: PostgreSQL Accessible
- CVE-2014-5063: Hardcoded Default Credentials

```
public PmDataConnector(String s)
{
    pConnector = null;
    type = graphTypes.E2E;
    pConnector = new PostgresConnector("jcostanza","jcostanza");
    pConnector.setServerAddress(s);
    pConnector.setPassword("shadow");
    startError = false;
    pmDataConnector = this;
    if(pConnector.openDatabase())
```

Logical: Production

- NTP
- PTP – not configured

Production: NTP

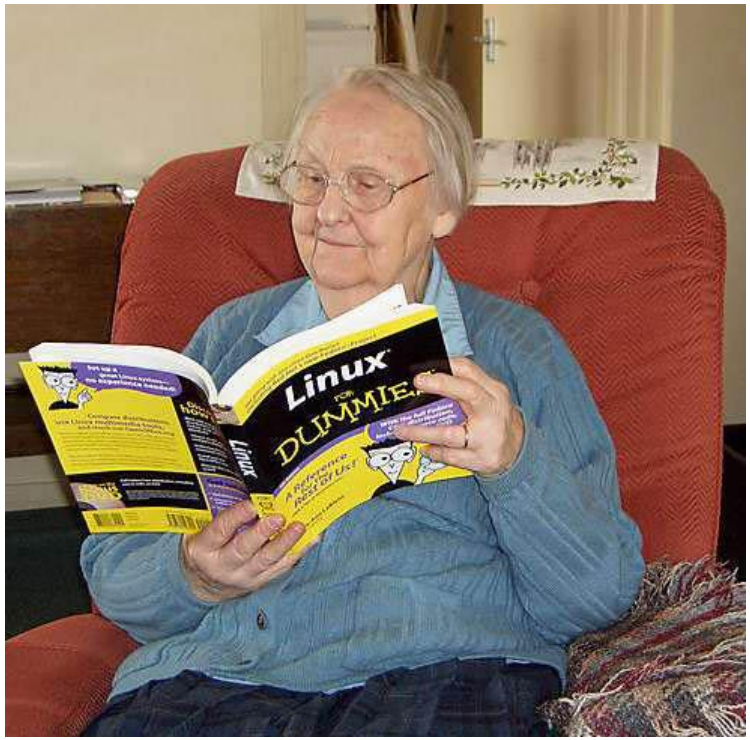
- MONLIST was enabled. Derp.
- What else were you expecting?

Logical: Authorised

- Safe to say we've owned the box
- Let's poke around...

Logical: Authorised

- CVE-2014-5066: World Writable Files & Directories
- CVE-2014-5065: Insecure Sudo Configuration



Ultimately Who Cares?

- Well, they do if they bought one
- All of us: The device we tested was being used to supply time to domestic appliances
- This guy:

  "FSMLabs or Symmetricom (although Symmetricom seem to have a habit of falling over unexpectedly and then being difficult to support/get new antennas for, at least in the UK). Avoid Meinberg unless you (like the rPi solution) like inaccuracies introduced by USB connected network adaptors." - El Reg Mole

fclose(presentation)

Twitter: @portcullislabs

Web: http://labs.portcullis.co.uk/