

## Re: SPRINT ADSL [Zyxel 645 Series Modem]

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-01/0040.html>

---

*From:* Jay Lagorio ([jay@LAGORIO.NET](mailto:jay@LAGORIO.NET))

*Date:* 01/27/03

Date: Sun, 26 Jan 2003 19:15:59 -0500

From: Jay Lagorio <[jay@LAGORIO.NET](mailto:jay@LAGORIO.NET)>

To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

It's terrible that this vulnerability can be used to get to a user's data at the same time by using it in conjunction with the poor security that is bound to plague the average home user's system. Telnetting into one of these things, then going to 24, 8, and 12 (the PING command), I can check for the existence of 192.168.1.2 on their network. If that doesn't seem to be there, I can always check the DHCP settings, in case they've changed the address the DHCP server will start assigning from. Then, back in the main menu, I can use option 15 (SUA Setup) to make the default NAT port forwarder (coming from the outside going inward) 192.168.1.2.

From there, if they don't have a username assigned to their computer, I can use mine and go to Start->Run and enter "\\<the-sprint-ip-address-here>". If they've left their password and such blank, and tweaked file sharing for their maximum convenience (IE, sharing the C Drive), I have access to their entire file system.

Pretty scary stuff, and all made possible thanks to the poor default password on the modem. IMHO, the config utility on Port 23, and web interface on Port 80, and the FTP server on Port 21 shouldn't be accessible from the WAN port unless it's explicitly turned on AFTER installation in the user's home - but that would require use of forward-thinking on the part of Zyxel. Unfortunately, their flaw has caused an untold number of people to be vulnerable to this bug, and a good portion of them won't ever have any idea that it exists. I'm sure many of that chunk of users don't know what the model on their modem is to begin with.

To take directly from their website:  
"Zyxel - Total Internet Access Solution"  
HA! They sure weren't kidding, were they?

--Jay Lagorio  
<http://www.lagorio.net>

-----Original Message-----

From: [http-equiv@excite.com](mailto:http-equiv@excite.com) [mailto:[http-equiv@MALWARE.COM](mailto:http-equiv@MALWARE.COM)]

Sent: Thursday, January 23, 2003 10:36 AM

To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

Thursday, January 23 2003

Sprint FastConnect[insert little registration r here]ADSL provides the Zyxel series of modem/routers to their customers. The problem is all these devices are factory set with default commonly known passwords and logins and include a little http, ftp and telnet server. This allows for remote configuration of the network settings and host of other things. Including uploading and downloading the modem configuration file rom-0, rebooting the modem, changing the modem's remote management login and password, various other "high- tech" fiddling possibilities. Through both telnet and web.

Certainly not of interest or of need to your generic subscriber.

Quick pretend examination of:

Sprint NETBLK-SPRINTBLK (NET-198-67-0-0-1) 198.67.0.0 - 198.70.255.255  
LTD SPRINT FLA ANS ISP FON-332652953698729 (NET-198-70-208-0-1)  
198.70.208.0 - 198.70.223.255

shows 800 out of 2000 [of 100,000 or so] affected modems. Closer examination confirms:

Copyright (c) 1994 - 2002 ZyXEL Communications Corp.

P645ME+ Main Menu

Getting Started Advanced Management

1. General Setup 21. Filter Set

Configuration

3. Ethernet Setup 22. SNMP Configuration

4. Internet Access Setup 23. System Password

24. System Maintenance

25. IP Routing Policy Setup

Advanced Applications 26. Schedule Setup

11. Remote Node Setup

12. Static Routing Setup

15. SUA Server Setup 99. Exit

Enter Menu Selection Number:

punching in on our replica modem, number four [4], we get:

Menu 4 - Internet Access Setup

NT-Bugtraq: Re: SPRINT ADSL [Zyxel 645 Series Modem]

ISP's Name= MyISP  
Encapsulation= PPPoE  
Multiplexing= LLC-based  
VPI #= 8  
VCI #= 35  
Service Name=  
My Login= grandpamalware@malware.com  
My Password= \*\*\*\*\*  
Single User Account= Yes  
IP Address Assignment= Dynamic  
IP Address= N/A  
ENET ENCAP Gateway= N/A

Press ENTER to Confirm or ESC to Cancel:

Press ENTER to Confirm or ESC to Cancel:

Playing with our replica modem a bit more we GET:

```
ftp> open malware.com
Connected to malware.com.
220 Sprint FTP version 1.0 ready at Wed Jan 5 17:20:47 2000 User
(malware.com:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp> get rom-0
200 Port command okay
150 Opening data connection for RETR rom-0
226 File sent OK
ftp: 16384 bytes received in 2.03Seconds 8.07Kbytes/sec.
ftp>
```

Due to our modem only being a replica, we are unable to determine whether uploading our custom crafted rom-0 file from our second replica modem to our first, will (a) register the user data from there to there inclusive of user name and password and or (b) overwrite the configuration file in such a way our modem then becomes useless.

But without a doubt, we are not happy to see Grandpappy's private email address out in the open for the whole world to see.

Notes:

1. The provider suggests that slapping up a web page with instructions to disable this "feature" will be the solution. We would suggest fire-walling off the entire affected user base ftp, http and telnet ports, rolling out the trucks, physically reconfiguring each and every affected subscriber's modem or replacing them
2. PRIVACY PRIVACY PRIVACY. In this day and age, it is all we have left !
3. <http://www.wired.com/news/infostructure/0,1377,57342,00.html>

Re: SPRINT ADSL [Zyxel 645 Series Modem]

4. Victims of this contact your provider as possible and have them hand-hold you through disabling this "feature". Better yet, insist they send over the installer to do it for you. After all it should have been done at time of installation.

End Call

--

<http://www.malware.com>

oo  
oooo

Delivery co-sponsored by TruSecure Corporation

oo  
oooo

TICSA - Anniversary Special - Limited Time

Become TICSA certified for just \$221.25 US when you register before 3/31/03 with PROMO "TS0103" at [www.2test.com](http://www.2test.com). NO membership fees, certification good for 2 years. Price for international delivery just \$296.25 US, with this offer. Offer cannot be combined with any other special and expires 3/31/03. Visit [www.trusecure.com/ticsa](http://www.trusecure.com/ticsa) for full details.

oo  
oooo

oo

Delivery co-sponsored by TruSecure Corporation

oo

TICSA - Anniversary Special - Limited Time

Become TICSA certified for just \$221.25 US when you register before 3/31/03 with PROMO "TS0103" at [www.2test.com](http://www.2test.com). NO membership fees, certification good for 2 years. Price for international delivery just \$296.25 US, with this offer. Offer cannot be combined with any other special and expires 3/31/03. Visit [www.trusecure.com/ticsa](http://www.trusecure.com/ticsa) for full details.

oo