(5)Severity – High DrayTek Port Redirection Stored XSS

Subject	DrayTek Port Redirection	on Stored	Severity	High
	XSS			
Category	Cross-site scripting		Target	X.X.X.X
Position	http://x.x.x.x:443			
Version	Firmware Version: 3.8.8.2			
Description	Attacker can inject malicious code in this page.			
Threats	When the Draytek admin login and visit the this page, it will			
	execute malicious code which attacker injected automatically			
	Then attacker will get the admin privilege and shell, it can			
	compromise the Draytek router and penetrate the intranet			
	compromise the Braytek router and penetrate the intranet			
Test	The vulnerability occur on "NAT"→"Port Redirection" page			
Procedures	Attacker can inject malicious code in this page			
	(C framework (specific 4) (S)) (C (
	Dray Tek Vigor 2912 Series ★ 1811 🖶 🖙			
	Off • IR6 NAT >> Port Redirection			
	Wizania Online Status			
	Online Status Mo	de	Single •	
	LAN	rvice Name stocol	141414141 TCP *	
	- CALL	NN Interface	ALL .	
	700000000000000000000000000000000000000	blic Port urce IP	Any •	IP Object
	Exc. Lorenze	vate IP	1.1.1.1	
	Firewall Note: User Management In "Range" M Objects Setting been entered	vate Port ode the End IP will be calculate	ed automatically once the P	Jublic Port and Start IP have
	CSM Bandwight Minus rement Applications VPN and Remote Access Certificate Management			
	Attacker can temper the parameter to malicious code			

