WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
MI424-WR Rev.E	Actiontec	Router	20.19.8	No	No	None	n/a	WPS "functionality" is not enabled currently	This is the type of router that is used for Verizon FIOS and it appears to me at least that despite there being a button for WPS on the outside of the box, Actiontec says in the user manual: "Although the WPS button is included on the FiOS Router, WPS functionality will not be enabled until a future firmware release. The button is included so that WPS can be activated at a later date without having to physically change the FiOS Router. The GUI does not include the WPS option."	00:1F:90	ajdowns		
WLAN 1421	Alice/Hansenet	Wlan Router	1.0.16	No	Yes	Reaver		Yes	I did a quick check. Seems to be vulnerable. But with some kind of rate limit maybe. Every second try fails.				
AirPort Extreme	Apple	Router	7.5.2	No	No	n/a	n/a	Yes, see comments	Apple seems to use the internal PIN Method, not external PIN.	60:33:4B	jagermo		
Vodafone Easybox 602	Arcadyan	Router/Modem	20.02.022	Yes	No	Reaver 1.3		Yes		0:23:08			Do we have more information about this? WPS PIN is enabled, but device is not vulnerable? Why?
Vodafone EasyBox 802	Arcadyan	Router/Modem	4/20/0207	Yes	Maybe	Reaver 1.3, WPScrack		Yes	The Router brings a Message after 10 failed logins: Warnung: Bedingt durch zu viele Fehlversuche, nimmt ihre EasyBox keine WPS PIN Registrierung von externen Teilnehmern mehr entgegen. Bitte setzten diesen WPS PIN durch einem neue zu generierenden WPS PIN Code wieder zuruck. Translation: Device locks after ten wrong attempts, user needs to create a new WPS PIN code	0:26:04			
Speedport W 504V Typ A	Arcadyan	Router	unkown	Yes	Yes	Reaver 1.4 r122	1 sek	yes		00:1D:19		12345670	
EasyBox 803	Arcadyan Technology Corporation	Router	30.05.211 (01.07.2011-10:36:41)	Yes	Yes	Reaver 1.3	[user reports untested, so his 3sec value here removed]	yes (not testet maybe its already ative after switching to off!)	i think there is an interesting thing between easyboxes and speedport AP's some esyboxe's use a standard key begins with spXXXXXXXXXXXXX with a 13 char length numeric key! (also some speedport aps use such a key but there is a nice script to get them with the hexdecimal mac of the target ap! [wardiving wiki!!!] that will work for a lot of speedport models ...) Have nice day CriticalCore	00:15:AF	CriticalCore		
RT-N16	ASUS	Router	1.0.2.3	Yes	Yes	Reaver 1.3	1176 seconds	Yes		bc:ae:c5			
RT-N10	ASUS	Router	1.0.0.8	Yes	Yes	Reaver 1.3	2 seconds per attempt/3.5 hours to crack	Yes			Reece Arnott		
N13U v1&v2	ASUS	Router	2/1/2012	No	No	Reaver 1.3	10min	Yes	ASUS N13U uses only PBC WPS configuration method . WPS is switched off automatically after two minutes . Tested on ASUS N13U v1 and v2 using latest firmwares		hA1d3R		
Fritz!box 7390	AVM	Router	84.05.05	No	No	will follow soon	will follow soon	Yes	I found this list at work and thought I can provide you with some information of my router. I filled out the parts I know and will check the clear field this evening: - Is your device vulnerable against the WPS attack? * - Wich tool did you use? * - How long did it take you?		FireFly		Hi Firefly, thanks - to fill in the missing informations, just re-do the form.
Fritz!Box 7240	AVM	Router	73.05.05	No	No	wpscrack, Reaver 1.2	uncrackable	yes		00:24:FE			
FritzBox7390	AVM	Router	ALL	No	No	Reaver 1.3	uncrackable	Yes	You have to activate WPS manually. I's deactivated after every successful wps connection and after 2 minutes. =>Not vulnerable because of very short time limit.		f.reddy		
Fritz!Box WLAN 3370	AVM	Router / Modem	103.05.07	No	No	N/A	N/A	Yes	I think all current AVM devices are save as WPS with pin isn't activated on default.				
n150	Belkin	Router	Unknown	yes	yes	Reaver 1.2	12.5 hours	yes					
F9K1001v1	Belkin	Router	F9K1001_WW_1.00.08	Yes	Yes	Reaver 1.3	7765 seconds	Yes					
F6D6230-4 v1000	Belkin	Router	1.00.19 (Apr 22 2010)	Yes	Yes	Reaver 1.3	20 min	yes	No lockout, no delay needed.	0:23:15			
F9K1001v1 (N150)	Belkin	Router	1.0.08	Yes	Yes	Reaver 1.3	41 minutes, 12 seconds	Yes	The F9K1001v1 is the same as the Belkin N150. I got lucky on the speed, the first 4 digits were found at 3.06% completion.	08:86:3B	Nick	21250491	
F7D1301 v1	Belkin	Router	1.00.22	Yes	Maybe	none		yes	didn't bother to test, but i assume it's vulnerable judging by the other Belkin routers that come with WPS enabled	94:44:52	beej		
F7D2301 v1	Belkin	Router	1.00.16 (Jul 2 2010 14:36:56)	Yes	Yes	Reaver 1.3	1.9 Hours	Yes		94:44:52		93645348	
F9K1105 v1	Belkin	router	1.00.03 (Jul 4 2011)	Yes	Yes	Reaver 1.3	3hours	yes					
F9K1001 v1	Belkin	Router	1.00.08	Yes	Yes	Reaver 1.2	11.2 Hours	Yes				8302441	
7800n	Billion	Router	1.06d	No	Maybe	Reaver 1.3	14 hours	Yes	Only vulnerable when WPS is enabled. Even though I had my attack laptop in the same room as my router, it still took 14 hours to find the PIN. Disabling WPS is completely effective.	00:04:ED			
BiPAC 7404VGPX	Billion	AP	6.23	Yes	Yes	reaver 1.3	3hours	no					
WZR-HP-G300NH	Buffalo	Router	Unknown	Yes	Maybe	Reaver via Backtrack	Within 1 hour	Yes	With WPS turned off reaver did nothing. With WPS on reaver is looking for the pin. This routers was bought and being used in Japan.				
WZR-HP-AG300H	Buffalo	Access Piont	dd-wrt v24SP2-multi build 15940	Yes	No	reaver 1.4		No but it starts locked	WPS is enabled by default and I cannot turn it off. However, Reaver reports that the state is locked at first try. Beacon packets sometimes show WPS (and thus appear in walsh), and other time WPS is not in beacon packets and thus is not reported by walsh. So far I am unable to break wps with reaver even using the known PIN. I've never actually tested to see if wps even works properly in the first place however.				
Linksys E4200 v1	Cisco	Router	1.0.03 (Build 14)	yes	yes	Reaver 1.2	1 second / attempt, no anti-flooding / blocking / delay	no	WPS LED blinking continuously during attack. Vulnerable with latest firmware, no way to disable WPS -> epic fail! Anonymous user 9308: I've also noticed that across 2 different linksys devices (don't have them on me now) the default WPS pin of 12345670 was the result of 2.5 and 6 hours cracking				
Valet M10	Cisco	Router	2.0.01	Yes	Yes	Reaver 1.2	5 hours	NO	A newer firmware is available (2.0.03), but the changes were fairly trivial according to the release notes.				

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
Linksys E4200	Cisco	Router	1.0.0.3	Yes	Yes	Reaver	4h	NO	Feedback by security@cisco.com "Issue has been identified and being worked on by product engineering. There is no ETA of a firmware release. Please continue to check support web page for the E4200v1. If you have E4200v2 you can use the auto firmware update to see if there is a new firmware update."				
Linksys E3200 v1	Cisco	Router	1.0.02	Yes	Yes	Reaver 1.3 & r58	24h	No	With 1.3, use the --ignore-locks option. With r58 and over, use --lock-delay 60. The router has a 60 seconds cycle with 3 PINs. I was lucky it went as fast, it could've taken a lot longer.	58:6D:8F	Socapex		
WRVS4400N	Cisco	Router	1/1/2013	No	No	none		not available					
UC320W	Cisco	Unified Communications	Current Version	yes	yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
WAP4410N	Cisco	Access Point	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
RV110W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
RV120W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP521W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP526W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP527W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP541W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP546W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
SRP547W	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
WRP400	Cisco	Router	Current Version	Yes	Yes				Reported by Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps		Cisco		
Linksys E1000	Cisco	Router	2.1.00 build 7Sep 21, 2010	Yes	Yes	Reaver 1.4	7/6/2012	No	Took aound 6.7hrs to recover the WPS Pin	C0:C1:C0	aBs0lut3z33r0		
Lynksis E3200 v1	Cisco	Router	1.0.03	Yes	Yes	Reaver 1.4		No	As stated by Cisco for firmware 1.0.03: - Added Enabled/Disabled feature for Wi-Fi Protected Setup in the web configuration - Added WPS lockdown feature Not true, still works great :) There is no new WPS lockdown, still 60s/3 pins. Anyone else can confirm this?	58:6D:8F	Socapex		
WRT320N	Cisco Linksys	Router	unknown	Yes	Maybe	Reaver 1.4	n/a	unknown	Reaver constantly outputs 'WPS transaction failed (code: 0x2)', indicating an "Unexpected timeout or EAP failure".				
WRT610N	Cisco-Linksys	Router	2.00.01.15	Yes	Yes	Reaver 1.4	24 hours	Not Sure			Chaos	12215676	
DIR-825	D-Link	Router	2.02EU	Yes	Yes	reaver	5h	Yes		00:18:e7:fb			
DIR-615	D-Link	Router	4,1	Yes	Yes	Reaver-1.1	ca. 1h 45min	Yes					
DIR-855	D-Link	Router	1.23EU	Yes	Maybe	Reaver 1.3	user reported 5 minute timeout on failed registration, unknown inducement threshold	yes					
DIR-655 vB1	D-Link	Router	2.00NA	Yes	Maybe	Wifi Analyzer (Android) v3.0.2		Yes		5C:D9:98		Can be user-generated	
DIR-300 (HV - B1)	D-Link	Router	5/2/2012	Yes	Yes	Reaver 1.3	4 Days	yes - can be completely deabled			Nsol		
DIR-300	D-Link	Router	"2.05"	Yes	Yes	Reaver 1.3	4 Days	yes			Nsol		
DIR-655 A3	D-Link	Router	1.22b5	Yes	Yes	Reaver 1.3	4.5hrs	Yes	Device ships with WPS enabled; I normally keep disabled; older 1.22b5 firmware since more stable. Allows you to specify a different WPS PIN; When enabled took approx 4.5 hrs to recover WPS pin and WPA2 password; Router constantly re-boots (approx every 30-50 PIN attempts) during this period and was also subjected to a denial of service. Reaver continues to try pins when router recovers using -L option. Can adjust Reaver timing settings for better results. Reaver 1.3 on BackTrack 5R1. Reaver thinks router is rate limiting (it is actually crashing); restarting Reaver or using -L allowed Reaver to continue checking pins almost immediately or as soon as the router rebooted itself.				
DIR-300	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-457	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-501	D-Link	Router	Current						tested and reported by D-Link directly		D-Link		
DIR-600	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-615 Rev D+ H	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-615 Rev. B	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-635 Rev B	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-645	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-652	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-655	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-657	D-Link	Router	Current	Yes	Yes			Yes	tested and reported by D-Link directly		D-Link		
DIR-815	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-852	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
DIR-855	D-Link	Router	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DAP-1360	D-Link	Access Point	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DAP-1522	D-Link	Access Point	Current	Yes	Yes			yes	tested and reported by D-Link directly		D-Link		
DIR-625	D-Link	Router	3,04	Yes	Yes	Reaver 1.4	4 hours	Yes	Hardware version (very relevant for some D-Link devices): C2 This is the first device that I've successfully recovered the PIN from!	00:1E:58			
DIR-615	D-Link	Router	2,23	Yes	No	Reaver 1.3	n/a	Yes	Hardware version B2. This device appears to enter a WPS "blocked" state after approximately 60 failed PIN attempts (consistently around 0.60% progress in Reaver). It does not unblock until a system reboot.				
DIR-628	DLink	Router/access point	11/1/2012	Yes	Yes	reaver 1.3	Didn't let it run	yes	I didn't bother letting reaver run until it cracked the PIN -- I just wanted to confirm that it was vulnerable, and that turning off WPS fixed it. Walsh listed it as vulnerable before turning off WPS, but not after.				
DWA125 with Ralink2870 / 3070	Dlink	USB	1	No	No	Reaver 1.4		i don't know					
DWA125 with Ralink2870 / 3070	Dlink	USB	1	No	No	Reaver 1.4		i don't know					
3G-6200nL	Edimax	Router	1.06b	No	No	N/A	N/A	Yes	Router has a Push Button to Enable WPS				Can you verify, that push button is the only method they are using?
ECB9500	Engenius	Wireless Gigabit Client Bridge	02.02.2009	Yes	Yes	Reaver 1.3 >	4 hours	Yes	More information about this can be found here: http://www.virtualistic.nl/archives/691		virtualistic.nl		
EchoLife HG521	Huawei	Router	1,02	yes	yes	Reaver 1.1	5-6 hours	yes	TalkTalk ISP UK				
BtHomeHiub3	Huawei	Router/ADSL	Unknown	Yes	Yes	Reaver 1.3	50 minutes	Unknown		Unknown			
E3000	Linksys	Router	1.0.04	Yes	Maybe - see Comments	Reaver 1.3	24h	Yes	WPS lockdown after 20 attemps (power cycle needed). Testet with reaver -p "PIN" ->got WPA Key. =>not vurlnerable because of automatic lockdown.	58:6D:8F:0A	f.reddy	69382161	more information about this router and the WPS-DoS: http://www.reddit.com/r/netsec/comments/nzvys/wps_brute_force_i_started_public_google_doc_so_we/c3domfn
WRT350N	Linksys	Router	2.0.3 i think (newest!)	Yes	Maybe - see Comments	Reaver 1.3		Yes	Reaver gives thousands of errormessages when I try to crack this type of AP. Tried several parameters... Strange WPS implementation!?!?	00:1D:7E:AD	f.reddy	66026402	

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
E2500	Linksys	Router	1.0.02	Yes	Maybe	Reaver 1.3	I stopped Reaver after 16 hrs with no success. See comments	No	I left Reaver running overnight, it was stuck in an error the next day after 16 hours. It kept trying to attempt to send a PIN, but every time it would return the error "[!] WARNING: Receive timeout occurred". The WPS LED on the back of the router is normally solid green; it starts to flash on and off during the attack, and when this error is hit the LED turns off and stays off. The only way to fix this is to unplug the router and plug it back in. I was only able to retrieve the pin after resetting the router a few times by unplugging/replugging it and restarting Reaver from where it left off.	58:6D:8F	Nick		
WRT120N	Linksys	Router	v1.0.01	Yes	Yes	Reaver 1.3	4h	no	had to restart the router after 29%, because reaver stuck at the same pin and received timeouts	00:25:9C			
WRT160Nv2	Linksys	Router	2.0.03	Yes	Yes	Reaver	5 hours	no					
E1000	Linksys	Router	unknown	Yes	Yes	Reaver 1.3	7h	No	2 seconds/attempt - I let it run all night, had a few hiccups (timeout warnings), but psk was eventually found.	c0:c1:c0			
E1200	Linksys	Router	1.0.02 build 5	Yes	Yes	Reaver 1.4	5 hrs, 20 mins	No	2 secs/attempt; Never locked up EVER!	58:6D:8F	Molito		
E4200	Linksys	Router	1.0.02 build 13 May 24, 2011	No	Yes	Reaver v1.3	4 hours	No, it doesn't appear to be		58:6D:8F	txag	47158382	
WRT54G2	Linksys / Cisco	Router	unknown	Yes	Yes	Reaver	6 hours	Yes, but not sure if it stays off	This information ist from this Arstechnica article http://arst.ch/s0i - filled in by jagermo - but it seems that Linksys does not have a standard-pin		Sean Gallagher	8699183	
E4200	Linksys / Cisco	Router	unknown	Yes	Yes	Reaver 1.3 - with PIN-Option		No, see comments	Confirmed that PIN-Method stays switched on, even if you turn WPS off in the management interface. This is really a problem.		jagermo		
WRT350Nv2.1	Linksys / Cisco	Router	2.00.20	Yes	Maybe	Reaver 1.4		No	Starts testing PINs and after 2 attempts I supose it lock you out. Testet with reaver -p "PIN" ->got WPA Key.		Inakiuy		
WAG160Nv2	Linksys by Cisco	ADSL Modem Router, Wifi AP	2.0.0.20	Yes	Yes	Reaver 1.4	5.5 Hrs	No. Though the router's web portal has an option to not choose WPS, it still remains active.	It took about 1.5 seconds per attempt when the router was not doing any activity, took around 5 hrs for the first half of PIN and few mins for rest. The Linksys WAG160Nv2 router doesn't have any lock down and no option to disable WPS either. The Router didn't crash and the PIN was cracked on first attempt, though the mon0 interface on BT5r1 crashed. The Reaver was started again with earlier instance. When the router was active with couple of wired and wireless users with LAN and Internet activity, it took about 40 seconds per attempt.		@_Niranjan		
WRT100	Linksys-Cisco	Router	1.0.05	Yes	Yes	Reaver 1.4	76 minutes	No	cracked PIN was not the same as the PIN displayed in the router's security settings. looks like pin can be customized but there is also a default PIN hard coded into the router.	00:1D:7E			
WRT100	Linksys-Cisco	Router	1.0.05	Yes	Yes	Reaver 1.4	76 minutes	No	cracked PIN was not the same as the PIN displayed in the router's security settings. looks like pin can be customized but there is also a default PIN hard coded into the router.	00:1D:7E			
NP800n	Netcomm	Wireless Router	1.0.14	Yes	Yes	Reaver 1.3	10 hours	yes		n/a	ISP rep		
CG3100	Netgear	Cable Modem (with built in Gateway/AP)	3.9.21.9.mp1.V0028	No	No	Reaver 1.2		Yes	This device has support for WPS, turned off by default, and only through the Push-Button and Registrar PIN method (i.e. enter the Wireless Adapters PIN at the AP side, as opposed to enter the APs PIN at the Wireless Adapter side)	c4:3d:c7			
CG3100D	NETGEAR	Cable/router	unknown	Yes	Yes	reaver svn rev. 52	5 hours	yes	Is a router provided by very popular ISP, at least in my country. Was tested with options: -r 5 -x 30 -w Signal was about -60 Sometimes reaver enters in a loop and tries the same PIN 10 or 15 times, but luckly continues as normal after these 10-15 tries.		gorilla.maguila@gmail.com		
DGND3700	Netgear	Modem/Router	V1.0.0.12_1.0.12	Yes	Yes	Reaver 1.3		Yes	Router has a timeout built in afet approx 20 attempts; using default delay (315 secs) will allow resume - but does significantly slow down the number of attempts/sec.	20:4E:7F			I'm seeing something similar on the WNDR3700
WNDR3700	Netgear	Router	1.0.7.98	yes	yes, but.... see comments	Reaver 1.2			Device locks after WPS Flodding, if you wait for like half an hour and use Reaver 1.3, you can resume the attack. Returns PIN, but WPA2-Passphrase is gibberish				
DGN1000B	Netgear	Router	1.00.45	No	Maybe	WPScrack		is deactivated by default	WPS is only enabled for approx. 2 min when you use push 'n' connect to connect a new device to WLAN.				
MBRN3000	NetGear	Router (ADSL + 3G)	1.0.0.43_2.0.11WW	Yes	Yes	Reaver 1.3	3h	yes			dankwardo		
WNDR3700	Netgear	Router	V1.0.7.98	Yes	Yes	Reaver 1.3	9hrs	yes					

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
DGN1000B	Netgear	Router	1.1.00.43	Yes	Maybe	reaver 1.2		No (there is a checkbox, but it's disabled)	I haven't got any WPS client, but reaver started guessing PINs so I assume that WPS is enabled by default. Anyway after 12 PINs there seems to be a rate limit with a timeout greater than 315 seconds. So I think it is possible to get the PIN but it would take much longer than 10 hours.	00:26:F2			
WNDR3700	NETGEAR	Router	v1.0.4.68	Yes	Yes	Reaver 1.3	est. 24h	unkown			Nsol		
WNDR3700v3	Netgear	Router	V1.0.0.18_1.0.14	Yes	Maybe	Reaver 1.3		PIN can be disabled, but WPS cannot be switched off completely	First test, with WPS PIN enabled: router was responding to PIN requests. Reaver was cycling through attempted PINs. I only attempted to attack the router for a few minutes, but it appeared Reaver would have found the PIN eventually. Second test, with WPS PIN disabled: router responded to PIN requests with a lock immediately. I allowed reaver to run for 2 hours and the lock never terminated. It appears the WPS PIN disable feature works as intented. I would prefer that Netgear would allow WPS to be disabled completely. WPS always has been a weaking of the wireless security to ease connections. I'm looking forward to DD-WRT becoming available for my router.				
CGD24G	Netgear	Cable Modem Router	unknown	Yes	Yes	Reaver 1.3	12 Hours	No	Router supplied by very large ISP in my country for all cable users.				
WGR614v8	Netgear	Router	1.1.11_6.0.36	Yes	Yes	Reaver 1.3	1 day	Yes, PIN can be locked out but WPS remains on	Factory/stock firmware 1.1.11_6.0.36 has a bug that revealed PSK after Reaver had obtained only the first 4 digits of the PIN. The router accepted PIN 16075672, but the correct PIN is actually 16078710.			16078710	
WGR614v8	Netgear	Router	1.2.10_21.0.52	Yes	Maybe	Reaver 1.3	1 day	Yes, PIN can be locked out but WPS remains on	Router locks down WPS PIN for ~5min after around 30 attempts, but only while Reaver was cycling the first four digits. Once the first four correct digits were found, the router did not lock down at all while reaver was cycling the last three digits.				
WNR1000 (N150)	Netgear	Router	unknown	Yes	Maybe	Reaver 1.3	n/a	Yes	"version 3" of this device. This device is vulnerable to a DoS condition, but seemingly not PIN disclosure. The router stopped providing connectivity to all clients after approximately two hours of testing, and service was not restored until the system was rebooted.				
WNR3500L	Netgear	Router	V1.2.2.44_35.0.53NA	Yes	Yes	Reaver 1.4	18hrs	Yes		20:4e:7f	blue team consulting		
WNR3500v2 (N300)	Netgear	Router	V1.2.2.28_25.0.85	Yes	Probably	-	-	Yes	Not yet tested, but siblings being vulnerable suggests exploitable over longer periods of time. To be tested soon.				
WNR200V2	Netgear	Router	v2	Yes	Yes	Reaver v4.0	24 hours	yes				90889301	
WNDR3700v1	NetGear	Router	1.0.16.98 - BETA	No	No	Reaver 1.4		deactivated by default	WPS is LOCKED by default with this firmware confirmed with WASH		grik		
DGND3300v2	Netgear	ADSL Router	2.1.00.52	Yes	Yes	reaver	under 3 hours	No	2.1.00.52 is a beta firmware that Netgear have not officially released. It allows the WPS Pin to be disabled - the 2.1.00.48 (latest available) firmware will not save the disabled setting. Even with the pin disabled the exploit will return the PIN and WPA password. Both 2.1.00.48 and 2.1.00.52 firmwares are exploitable.		@RiseKB		
WNR1000 (N150)	Netgear	Router	V1.0.2.28_52.0.60NA	Yes	Maybe	Reaver 1.4	< 1 Day	Yes	The PIN was a high number, so the attack would take some time due to the brute force method. If you run reaver with no/little delay, the AP would lock you out for quite some time. Using the "-d 7" argument, I was able to try pins continuously without being locked out. A suggestion would be to start at given PIN ranges, for either/both of the first 4 and last 4 digits.			7097xxxx	
WNR3500V2	Netgear	Router	V1.2.2.28_25.0.85	Yes	Yes (though does slow down attack considerably)	n/a	n/a	Yes	See http://support.netgear.com/app/answers/detail/a_id/19824 for Netgear's response and recommendation about this.				
WNR3500V2	Netgear	Router	V1.2.2.28_25.0.85	Yes	Yes (though does slow down attack considerably)	n/a	n/a	Yes	See http://support.netgear.com/app/answers/detail/a_id/19824 for Netgear's response and recommendation about this.				
F@st 3504	Sagem	Router	Bbox firmware - 8.4.M.O (not sure)	Yes	Yes	Reaver 1.3	More than 5h	Unknown					
SX763	Siemens Gigaset	Router/Modem	4.3.52.21.07	Yes	Yes	Reaver 1.3	45 minutes	Yes	It was crawling slowly for 40 mins until it jumped from ~5% to 91% and then to 100% in a minute or two.	0:21:04	neuromancer		
Sitecom 300N WL-363	Sitecom	Router/Modem	2.00.01	Yes	Yes	Reaver 1.4	2~3 hours	Yes					

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
Speedport w720v	T-Online	Router	1.61.000	No	No	Reaver 1.1	-	No (A 2-Minute-Interval Button is used)	-	00-1D-19			
Speedport W 723V	T-Online	Router	1.00.080	Yes	Yes	Reaver r65	2-3 hours	yes	Wireless Chipset: Atheros AR5001X+ Driver: ath5k	84:A8:E4			
TG784n	Thomon	Router	8.4.H.F	Yes	Yes	Reaver 1.4	3 days? (needs more testing)	Yes (Please correct This)	Please correct last comment, WPS can be disabled on ALL thomson routers by telnet. Guide to do so here: http://npr.me.uk/telnet.html		Snayler		
TG784	Thomson	Router	8.4.2.Q	Yes	Yes	Reaver 1.3	15 hours	unkown	Used reaver 1.3. Crucial to use the flags -E -L and adjust the timeout (-t) to be greater or equal than 2 seconds.				
TG782	Thomson	Modem/Router	8.2.2.5	Yes	Yes	Reaver 1.3	24h	Probably no	Used Reaver 1.3. Took quite a few hours to break with many error messages like "receive timeout occurred" and "re-transmitting last message". The attack was slow like 4-30sec/attempt but the result was good. Couldn't find any settings to disable WPS...				
TG784n	Thomson	Router	8.4.H.F	Yes	Yes	Reaver 1.3	18hours	maybe	This router uses a firmware modded by the ISP so is no upgradable. Using JTAG its possible to turn off the WPS but needs some knowledge. The router uses a button to unlock the WPS feature by I run the attack without pressing it so its useless. I used this tags: -E -L -T 2	08:76:FF	MG		
TL-WR1043ND	TP-Link	Router			Yes	WPScrack			Video: http://vimeo.com/34402962				
TL-WR2543ND	TP-Link	Router	3.13.6 Build 110923 Rel 53137n	Yes	Yes, see comment	Reaver 1.2		yes	WPS-Service seems to lock down after 12 attempts, Restart required. If you crack the code in this time or if you add the key to the tool, it can be cracked	f8:d1:11	@jagermo		
TL-WR1043N	TP-Link	Router	3.12.2 Build 100820 Rel.41891n	Yes	Yes	Reaver 1.1	5h	Yes	Nice work guys...	F4:EC:38	Mannheim	26599625	
TL-WR2543ND	TP-Link	Router	3.13.4 Build 110429 Rel.36959n	Yes	Yes	Reaver 1.3	8h	yes		F4-EC-38	prslss		
TD-W8950ND	TP-Link	Router,Bridge, Modem	1.2.9 build 110106 Rel.59540n	Yes	Yes	Reaver	30 Minutes	Yes.But Reaver still gets in.	Reaver got in in 30 minutes on a basic adapter with no injection,but it actually took LONGER when using an ALFA injection card...	00:0C:F1	TheDarkGlove96	30447028	
TL-MR3420	TP-LINK	Router	3.12.8 Build 110418 Rel.43954n	Yes	Yes	Reaver 1.4	10 hours	yes	Just add the flag -L and whait :)		cenoura		
WR841N	TP-Link	Router	3.10.4 Build 100326 Rel.42446n	Yes	Yes	Reaver	3 Hours	Yes	Called QSS instead of WPS				
TL-WR841ND	TP-Link	Router	3.10.4 Build 100326 Rel.42446n	Yes	Yes	Reaver	3 Hours	Yes	Called QSS instead of WPS				
WR841ND	TP-Link	Router	3.10.4 Build 100326 Rel.42446n	Yes	Yes	Reaver	3 Hours	Yes	Called QSS instead of WPS				
TL-WR841N	TP-Link	Router	3.10.4 Build 100326 Rel.42446n	Yes	Yes	Reaver	3 Hours	Yes	Called QSS instead of WPS				
TL-WR740N	TP-LINK	Router	3.12.4 Build 100910 Rel.57694n	Yes	Yes	Reaver 1.4	3h	Yes	Called QSS instead of WPS				
EVW3200	Ubee	Router/Modem	unknown	Yes	Yes	Reaver 1.4	6-8 hours	No	Run reaver with option --no-nacks				
XWR100	Vizio	Router	1/1/2002	Yes	Maybe	Reaver 1.2	N/A	No, see notes	Router appears to lockdown and disable WPS after approximately 20 failed attempts. Power cycle reenables. Not sure if WPS will reenable automatically after some unknown time period. I waited a few hours and it did not reenable.	0:27:22			
P-660W-T1 v3	ZyXEL Corporation	Modem/Router	V3.70(BRI.2) | 02/09/2011	Yes	Yes	Reaver 1.3	3hours (stopped at 31,75%)	yes	It was a slow attack, about 2 seconds/attempt The WPS feature could be easily deactivated and changed.	50:67:F0	MG	20064525	
TALKTALK-F03653		Router/Modem	Unknown	Yes	Yes	Reaver 1.2	1 hour	yes	TalkTalk ISP UK				
F9K1002	Belkin	Router	F9K1002_WW_1.00.08	Yes	Yes	reaver 1.4	~5 hours	yes`	Using the --dh-small option in reaver results in a M4 NACK even with the correct pin.	08:86:3b	subhuman	3737xxxx	
WTM652	Arris	Router / Access Point	1228	Yes	Yes	Reaver 1.4	12 Hours	Maybe					
SMC7901WBRA2	SMC	ROUTER/MODEM (ADSL2+)	1.0.3.1	Yes	Yes	Reaver 1.4	9 seconds	Yes, see comments	Even though it's not advertised as having this feature, this router comes with WPS activated by default with common 12345670 pin code! Although WPS doesn't show a menu tab on WLAN settings (firmware v1.0.3.1), it's possible to disable it by linking directly to that (hidden) setup page at http://192.168.2.1/admin/wlwps.asp Used arguments:reaver -i mon0 -b 00:22:2D:**:**:** -vv	00:22:02	luicci	12345670	
SMCWBR14-N2	SMC	Router	1.0.6.0	Yes	Yes	Reaver 1.4	3729sec=62min=1 hour	Yes	You may effectively disable WPS on "advanced">"wi-fi protected setup" router's page. Used arguments:reaver -i mon0 -b 00:13:F7:**:**:** -vv -d 0 -S	00:13:F7	luicci	14755989	

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
F@ST2864	Sagem	Modem/Router	FAST2864_v66396	**Yes**	Yes	Reaver	2hrs			c8:cd:72		1E6DFE19	
ADSL2+ Wi-Fi N	Telecom Italia	Modem	AGPWI_1.0.3	Yes	Yes	Reaver 1.4 (pins.c modified)	3 hours		pin doesn't respect the "checksum" rule for last digit. I implemented a simple exhaustive method under reaver/src/pins.c once pin is found reaver can't retrieve PSK. using wpa_supplicant & wpa_cli it is possible to retrieve PSK. from this moment AP disable completely WPS. I can still connect with AP using psk without problems. wash and reaver don't see the AP anymore. Retrieving psk with wpa_cli and wps pin doesn't work anymore. aireplay-ng doesn't fakeauth anymore (it used to work with this AP during the use of reaver) and give this message: Denied (code 12), wrong ESSID or WPA?	D4:D1:84:DB:35:6B	stefano.orsolini (gmail.com)	1234567	
DIR-615			D-LINK		Yes	Reaver 1.2							
F6D4230-4 v3 (01)	Belkin	router	3.00.03 Jun 29, 2009	Yes	Yes	Reaver 1.4	several hours			00:23:15	Mark		
WNDR4500	NETGEAR	Router	1.0.1.20_1.0.40	Yes	Maybe	Reaver 1.4			After 3 failed attempts pin automatically disabled and Reaver could not continue the attack.	84:1B:5E	trev.norris		
WNDR3700	Netgear	Router	unknown	Yes	Yes	Reaver 1.4	15h		Attack worked better without -S switch. Used DWA-140 (RT2870) for attack.				
TG862G	Arris	Cable Modem Gateway	unkown	Yes	Yes	Reaver 1.4	Pin cracked in 34826 seconds	unknown				81871452	
DIR-615	D-LINK	Router	04.01.2014	Yes	Yes	Wifite				34:08:04		5389xxxx	
DIR-615	D-LINK	Router	04.01.2014	Yes	Yes	Wifite	5h	maybe	used wifite-2.0r85	34:08:04	wpsguy	5389xxxx	
TG585 v7	Thomson	ADSL Modem / Router	8.2.23.0	Yes	Yes	Reaver 1.4	A few days		Rate limiting is active on this modem/router. After 5 pin attempts, it locks you out for 5 minutes. This is a problem as it works out at about 70 seconds per pin attempt, and is therefore very slow. However, it can be cracked if you are patient. I tried all sorts of combinations of delays to try and avoid the timeout but couldn't find the sweetspot. Interestingly, WPS Pin attempts are not flagged in the "intrusion detection" logs which are enabled by default. I believe WPS can be turned off via telnet (I have not tried), but there is no option to do so in the user interface.	00:24:17	Alasala	84207302	
LW310V2	Sweex	Wireless Router	I2_V3.3.5r_sweex_01	Yes	Yes	Reaver	4 hours			00:16:0A	T. Crivat	22640086	
SMC8014WN	SMC Networks	Router	unknown	Yes	Yes	Reaver 1.4	6 hours			00:22:02			
WNR3500L	Netgear	Router	unknown	Yes	Yes	Reaver	2 days						
WAP-5813n	Comtrend	Router	P401-402TLF-C02_R35	Yes	Yes	Reaver 1.4	5782 seconds		This router is delivered by the Movistar company for optical fiber (FTTH) service. In this video: http://youtu.be/NA6zO5NBYes I show the vulnerability theory of Wifi Protected Setup, referring to padlocks to clarify the understanding, and practice is under Kali Linux on the same router (Comtrend WAP-5813n)	00:1A:2B	Gerard Fuguet	16495265	
WAP-5813n	Comtrend	Router	P401-402TLF-C02_R35	Yes	Yes	Reaver 1.4	5782 seconds		This router is delivered by the Movistar company for optical fiber (FTTH) service. In this video: http://youtu.be/NA6zO5NBYes I show the vulnerability theory of Wifi Protected Setup, referring to padlocks to clarify the understanding, and practice is under Kali Linux on the same router (Comtrend WAP-5813n)	00:1A:2B	Gerard Fuguet	16495265	
WNR2000v3	netgear	router	1.1.1.58	Yes	Yes	reaver 1.4	36 hours			4C:60:DE		31836289	
wnr2000v2	netgear	router	1.2.0.4_35.0.57NA	Yes	Yes	reaver 1.4	12 hours	unknown		30:46:9A		38940972	

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
F5D7234-4 v5	Belkin	router	05.01.2014	Yes	Yes	reaver 1.4	19 hours			08:86:3B		76726446	
WNDR3400v2	netgear	Router	unknown	Yes	Yes	reaver 1.4	18 hrs			84:1B:5E		29167012	
WNDR3700V4	netgear	Router	01.01.1932	Yes	Maybe	reaver 1.4			Under the check box to enable WPS it has another check box that says: "To prevent PIN compromise, auto disable the PIN after __ failed PIN connections, until router reboots. In auto disabled mode, router's WPS LED will keep blinking slowly" This is set to on by default but could be turned off manually thus making the device vunerable to attacks. I get a speed of about 5 secs/pin on this setting. These settings can be found under advanced>advanced setup>Wireless Settings>WPS settings	28:C6:8E	gottalovebrando		
HG256	Huawei	Huawei	V100	Yes	Yes	Reaver 1.4	7 hours	Yes	12 seconds/pin with good signal strength	82:7D:5E	weiyang		
ESR300H	EnGenius	Router	1.3.8.27	Yes	Yes	Reaver v1.4	6.5 hours	Yes	WPS can be disabled through router web interface. Appears to disables all WPS functionality.	00:02:06	mpickard		
TL-WR740N	TP-LINK	Router	3.16.5 Build 130329	Yes	Maybe	Reaver v1.4	NA	Yes	WPS is identified as QSS on this model. Firmware version 3.16.5 has multiple releases - Mar 22, 2013 (Build 130322) and Mar 29, 2013 (Build 130329) - same behavior with both builds. Router disables PIN after 10 failed attempts for the device. Re-enable through the web interface or reboot the router to reactivate PIN interface. PIN can be disabled through web interface, but doesn't retain disabled state through reboots unless WPS is deactivated.	f8:1a:67	mpickard		
EA4500	Cisco	Router	2.1.39.145204	Yes	Maybe	Reaver v1.4		Yes	router starts to block (AP Rate Limiting) after first 3 attempts for increasing periods of time.	c8:d7:19	mpickard		
unknow			unknow	No	Yes	Reaver 1.4		no	Give me a password	B0:48:7A:B2:F0:96	Kamal	54335677	
WNDR3300	netgear	router	1.0.45_1.0.45NA	Yes	Yes	reaver 1.4	37 sec/pin	yes		00:24:B2	Brand~o	37449858	
WNDR3400v2	Netgear	Router	1.0.0.38_1.0.61	Yes	Yes	Reaver	29.62 Hours. (106632 Seconds)	No	The router still had the default login information (admin/password). First time cracking a WPA password and it literally took almost forever! It took 29.62 hours! Just crazy! But hey, it worked!	84:1B:5E	Youtube- MasterCookiez	73312055	
WR-741nd	TP-Link	modem	v2	Yes	Yes	reaver		yes					
DIR-615	dlink	Router	04.01.2014	Yes	Yes	reaver 1.3	23963 seconds	didnt try it	i took a long time, because i have a signal of -79db.	00:24:01	Lokke	45558221	
SAMSUNG D7000	Samsung	SMART TV	1027	No	Yes	Reaver 1.4	5 seconds	Disable SWL	Enabling Samsung Wireless Link on the TV makes it an Access Point and gateway to the Internet and LAN. I wrote up my findings here: http://jumpingspider.co.uk/?p=646	E4:E0:C5	JEH	0	
WNDR3400v2	NETGEAR	Router	V1.0.0.38_1.0.61	Yes	Yes	Reaver 1.4	24+ hours	Yes	Locks after 3 failed attempts until reboot. WPS can be turned off completely.	2C:B0:5D			
Comments and background information start here	Want to add a device? Please use http://bit.ly/1pxFaqy		This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.	Want to add a device? https://docs.google.com/spreadsheet/viewform			Stefan Viehböck Research and WPScrack:						
Another Disclaimer: These entries are not verified - we simply don't have enough tests and devices (yet). So, please, don't base your PHD on it or anything...							http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/						
							Craig Heffner Blog Entry and Reaver:						
			Reddit-Link to discuss stuff:				http://www.tacnetsol.com/news/2011/12/28/cracking-wifi-protected-setup-with-reaver.html						

WPS Flaw Vulnerable Devices

Device Name	Manufacturer	Type (Router/ AP /Bridge...)	Firmware-Version	WPS enabled by default?	Vulnerable (yes/no)	Tool (Version)	Average time for penetration *without* providing the PIN	WPS can be disabled (and it stays off!)	Comments/Notes		tested by	PIN	This database is intended as an educational resource for users interested in IT-Security. I did not find the vulnerability, that honor goes to Stefan Viehböck and Craig Heffner.
			http://www.reddit.com/r/netsec/comments/nzvys/wps_brute_force				Theiver, fork of Reaver:						
							http://code.google.com/p/theiver/						
			want to talk about this? Please do and use the hashtag #WPSDoc				Dan Kaminsky collects WPS-data in Berlin:						
			want to contact me? @jagermo on twitter or jagermo@hushmail.com				http://dankaminsky.com/2012/01/02/wps/						