

Wireless Access Point: Wire-side security testing

Contents

Wireless Access Point: Wire-side security testing	1
Contents	1
Notes	2
Best and Worst	3
Among the most secure products in this test	3
Among the most insecure products	3
3Com WL-450 Access Point	4
High Risk Issues	4
Medium Risk Issues	4
Low Risk Issues	4
Actiontec GT701 Access Point	5
High Risk Issues	5
Medium Risk Issues	5
Low Risk Issues	5
Airespace 4000 wireless switch	6
High Risk Issues	6
Aruba 800 wireless switch	7
High Risk Issues	7
Medium Risk Issues	7
Low Risk Issues	7
Belkin F5D7230 Access Point/Router	8
High Risk Issues	8
Medium Risk Issues	8
Low Risk Issues	8
Buffalo WBR2-G54 Access Point	9
High Risk Issues	9
Medium Risk Issues	9
Low Risk Issues	9
Installer's Notes	9
Cisco 1100 Access Point	10
High Risk Issues	10
Medium Risk Issues	10
Low Risk Issues	10
Compex NetPassage WPE54G-SMA Access Point	11
High Risk Issues	11
Medium Risk Issues	11
Low Risk Issues	11
HP ProCurve 520wl dual radio Access point	12
High Risk Issues	12
Medium Risk Issues	12
Low Risk Issues	12
Linksys WAP54G Access Point	13

High Risk Issues	13
Medium Risk Issues	13
Low Risk Issues	13
Netgear WG302 Access Point	14
High Risk Issues	14
Medium Risk Issues	14
Low Risk Issues	14
Netopia 3347W Access Point and DSL router	15
High Risk Issues	15
Medium Risk Issues	15
Low Risk Issues	15
Proxim AP-4000 Access Point	16
High Risk Issues	16
Medium Risk Issues	16
Low Risk Issues	16
SMC SMC2555W-AG Access Point	17
High Risk Issues	17
Medium Risk Issues	17
Low Risk Issues	17
Trapeze Mobility Exchange 20 wireless switch	18
High Risk Issues	18
Medium Risk Issues	18
Low Risk Issues	18

Notes

- As with any penetration report, it is important to note that these boxes were scanned at a certain point in time, configured to as near to factory default settings as we could get them to the best of our knowledge. Depending on your configuration, your test results will vary.
- “The installer” is a reference to Network World Lab Alliance member Joel Snyder, the primary tester responsible for setting up the test bed.
- High Risk issues raised in this report are items that should definitely be addressed before installing this equipment into a production network, no matter what security concern level you have.
- Medium Risk are items that need to be addressed before installing this equipment in an high risk network, such as in a bank or an e-commerce site, where security concerns are a major priority.
- Low Risk are items that present possible vulnerabilities but the probability is low they will be exploited.

Best and Worst

Among the most secure products in this test.

Cisco 1100 Access Point, Compex NetPassage WPE54G-SMA Access Point, Linksys WAP54G Access Point, Netopia 3347W Access Point and DSL router, Proxim AP-4000 Access Point and Trapeze Mobility Exchange 20 wireless, for all of which we found few security flaws.

Among the most insecure products.

- 3Com WL-450 Access Point with Wind River VxWorks debugger port open and a management user interface that allowed the possibility to configure the device for access with no password at all.
- Actiontec GT701 Access Point with a management user interface that allowed the possibility to configure the device for access with no password at all, and was so brittle it reset itself when we ran a port scan against it.
- Belkin F5D7230 Access Point/Router with no password possible.
- Buffalo WBR2-G54 Access Point with no password possible.
- HP ProCurve wl dual radio Access Point with Wind River VxWorks debugger port open.
- Netgear WG302 Access Point with multiple potentially vulnerable services.
- SMC SMC2555W-AG Access Point with Wind River VxWorks debugger port open.

3Com WL-450 Access Point

High Risk Issues

1. The AP is configured with a username of 'admin' and no password. I was able to telnet into it. While this setting was a conscious choice by the installer, the product should not have allowed a blank password.
2. The AP's Web user interface clearly explains the default username is 'admin' with no password.
3. The Wind River VxWorks debugger port (wdbRPC, port 17185) is enabled. This might be accessed by an attacker, and is never needed for production use.

Medium Risk Issues

The AP uses Telnet and HTTP for access in the default configuration, rather than SSH and HTTPS (HTTP over TLS.) Installers note: You can disable HTTP and use HTTPS, but there is no secure alternative to using Telnet.

Low Risk Issues

All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Actiontec GT701 Access Point

High Risk Issues

1. The Web interface was active with no password. The fact the product is capable of exhibiting this behavior is a serious security flaw.
2. The act of scanning this AP reset the device to the factory defaults, so this devices is vulnerable to simple port scans.
3. The default command line (telnet) password ('admin') cannot be changed or disabled from the GUI

Medium Risk Issues

The AP uses Telnet and HTTP for access, rather than SSH and HTTPS (HTTP over TLS.)

Low Risk Issues

1. The AP responded on the UPNP UDP port, which should not be needed by an AP.
2. The AP responded on the DNS UDP port, which should not be open.
3. The AP responded on the RADIUS UDP port. The AP should not be acting as a RADIUS server from the wire side, only from the wireless side, so this is an unnecessarily open port.
4. All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Airespace 4000 wireless switch

High Risk Issues

1. The SSH implement used is OpenSSH 3.6.1p2. There are known vulnerabilities in that version of OpenSSH (see www.openssh.com). This version may be vulnerable.

Low Risk Issues

1. All possible ports respond to a UDP port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak..
2. All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Installer's Note Notes

- You can individually enable/disable whether or not the switch is manageable over the wireless network, which is a good thing.
- You can provide your own SSL certificate, which is much safer than using a self-signed certificate (which could be spoofed.)

Aruba 800 wireless switch

Medium Risk Issues

1. HTTP is used in the default configuration.
2. The HTTPS interface uses a self-signed certificate, which is vulnerable to man in the middle attacks.

Low Risk Issues

1. Telnet is used. It's only a stub server but it is still responding.
2. TCP ports QOTD, MYSQL, 4343, 8080, 8082, 8082 are open and are not needed for an AP.

Installer's Notes

- This device was not configured in the default secure mode the vendor recommends. The scan should be re-run with the default configuration.
- There is a full stateful firewall, which must be configured from the command line.
- Since this product also implements PPTP and IPsec and is a switch too, it has other ports open that you wouldn't expect to see in a plain AP.
- Our scan originally turned up a potentially vulnerable version of OpenSSH. However, the OpenSSH version reported by the product during the scan is, in fact, incorrect. The vendor has stated the code has been patched. The vendor will change the banner in a future release to use the "comment" feature of the IETF draft standard for SSH revision strings to indicate it has been patched.

Belkin F5D7230 Access Point/Router

High Risk Issues

It is possible, according to the GUI, to operate the AP with no password. In fact, this is the default configuration.

Medium Risk Issues

The AP uses HTTP for access, rather than HTTPS (HTTP over TLS) and it is not possible to change this.

Low Risk Issues

The following protocols were found by a port scan, all of which should not be present in an AP: 31 (MFE-NSP), 88 (EIGRP), 120 (UTI), 122 (SM), 210, 213

Buffalo WBR2-G54 Access Point

High Risk Issues

1. The Web interface was active with no password in its default production configuration.
2. The password, when set, has a maximum of 8 characters. This is short enough that current state of the art password cracking tools could be used to break into the AP.

Medium Risk Issues

1. It was possible to guess the password by repeated failed attempts to use the GUI. This should have been blocked after approximately 3 attempts, or at least slowed down.
2. The AP uses HTTP for access, rather than HTTPS (HTTP over TLS.)

Low Risk Issues

1. The AP responded on the DNS TCP port, which should not be needed by an AP.
2. The AP responded on TCP/2601 (Zebra), TCP/2602 (RIPD), and UDP/520 (ROUTE), even though the routing capability was not switched on in this specific configuration.
3. The AP responded on UDP/2048, an unknown port that should not be needed by an AP.
4. All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Installer's Notes

This product can do routing, so when that feature is turned on the routing protocol ports should be open.

Cisco 1100 Access Point

High Risk Issues

None found.

Medium Risk Issues

1. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible.
2. The AP uses Telnet and HTTP for access in the default configuration, rather than SSH and HTTPS (HTTP over TLS.) You can disable Telnet.
3. You cannot use HTTPS for the Web management GUI.

Low Risk Issues

1. The AP responded on the DHCP Server UDP port. Since this is only a wireless AP and not a switch, it should never be responding on the DHCP port on the wire side, even if the DHCP feature is enabled for wireless use.
2. The AP responded on the NTP UDP port, which should not be needed by an AP.
3. The following protocols were found by a port scan, all of which should not be present in an AP: 53 (SWIPE), 55 (MOBILE), 77 (SUN-ND)

Compex NetPassage WPE54G-SMA Access Point

High Risk Issues

None found.

Medium Risk Issues

1. The AP uses Telnet and HTTP for access, rather than SSH and HTTPS (HTTP over TLS.)

Low Risk Issues

1. The AP responded on UDP/2048, an unknown port that should not be needed by an AP.
2. The AP responded on the IGMP protocol, which should not be open on an AP.

HP ProCurve 520wl dual radio Access point

High Risk Issues

1. The Wind River VxWorks debugger port (wdbRPC, port 17185) is enabled. This might be accessed by an attacker.

Medium Risk Issues

1. The AP uses Telnet and HTTP for access by default in the production configuration. HTTPS was enabled but did not work.
2. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible. Furthermore, you don't need a username, so an attacker would only have to guess the password, not the password and username, making it even easier.

Low Risk Issues

1. The AP responded on the DHCP Server and Client UDP ports, which should not be needed by an AP on the wire side.
2. All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Linksys WAP54G Access Point

High Risk Issues

None found.

Medium Risk Issues

1. The management interface only uses HTTP, and can't be configured for HTTPS.
2. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible.
Again there is only a password and no username, which makes a guessing attack easier.

Low Risk Issues

The AP responded on the protocol 16 (CHAOS) and 42 (SDRP), which should not be open on an AP.

Netgear WG302 Access Point

High Risk Issues

1. vsftpd 1.1.3 is used. There are known vulnerabilities in vsftpd. This version may be vulnerable.
2. The SSH implement used is OpenSSH 3.6.1p2. There are known vulnerabilities in that version of OpenSSH (see www.openssh.com). This version may be vulnerable.

Medium Risk Issues

1. The AP implements FTP, which uses clear text passwords and should not be needed on an AP. Furthermore, the username and password is the same as that used on the administrative account, so if you used FTP you would be transmitting the administrative password unencrypted.
2. The AP implements HTTP, which should be turned off. It does redirect request to HTTPS, but this still means there is an HTTP protocol processor, and therefore a hacker could try to attack it.
3. The AP uses for HTTPS a self-generated (2-layer) CA/cert that is not verifiable and therefore subject to man in the middle attacks.
4. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible.

Low Risk Issues

1. The AP responded on the NETBIOS UDP port, which should not be needed by an AP on the wire side.
2. The AP responded on ports 1024 and 1025, which should not be needed by an AP.

Netopia 3347W Access Point and DSL router

High Risk Issues

None found.

Medium Risk Issues

1. The AP uses Telnet and HTTP for access, rather than SSH and HTTPS, and you cannot disable these and you cannot enable SSH or HTTPS.
2. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible.

Low Risk Issues

1. The AP responded on UDP/DNS, which should not be needed by an AP.
2. The AP responded on the UPNP UDP port, which should not be needed by an AP.

Proxim AP-4000 Access Point

High Risk Issues

None found.

Medium Risk Issues

- 1.
1. The AP uses Telnet and HTTP for access by default in the production configuration. HTTPS was enabled but did not work.
2. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible. Furthermore, you don't need a username so an attacker would only have to guess the password, not the password and username, making it even easier.

Low Risk Issues

1. The AP responded on the DHCP Server and Client UDP ports, which should not be needed by an AP on the wire side.
2. All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

SMC SMC2555W-AG Access Point

High Risk Issues

1. The Wind River VxWorks debugger port (wdbRPC, port 17185) is enabled. This might be accessed by an attacker.

Medium Risk Issues

1. The AP uses Telnet and HTTP for access, rather than SSH and HTTPS (HTTP over TLS.) In fact SSH and HTTPS are not available.
2. The password retry mechanism with telnet gives feedback on what usernames are valid (admin is valid, adm is not, for example). This leaks information.
3. It was possible to try multiple passwords for the HTTP interface without the UI responding with a delay, so a brute force password attack might be possible.

Low Risk Issues

All possible protocols respond to an IP protocol level port scan. This implies a simplistic filtering mechanism is used for firewalling off unwanted traffic and that might be weak.

Trapeze Mobility Exchange 20 wireless switch

High Risk Issues

None found.

Medium Risk Issues

1. The AP enables multicast protocols, possible for intra-AP communications. The use of multicast may be spoofable or disruptable thus causing a DoS.

Low Risk Issues

1. The AP responded on the UPNP UDP port, which should not be needed by an AP on the wire side.

Installers note: You can provide your own SSL certificate, which is much safer than using a self-signed certificate (which could be spoofed.) With Trapeze, the default configuration does not use a self-signed certificate.