EXECUTIVE SUMMARY

Home networks as well as many small offices commonly rely on consumer wireless routers to act as Internet gateway, firewall, access point, and Network Attached Storage (NAS) all rolled into one. A Tripwire research study of 653 IT and security professionals and 1,009 employees working remotely, found that critical security vulnerabilities are endemic across the entire Small Office/Home Office (SOHO) wireless router market. Used extensively in SOHO environments, these routers are frequently left unprotected by users, who often do not utilize even basic security controls that can protect the routers from attack.

Tripwire’s Vulnerability and Exposure Research Team (VERT) analyzed the security provided by the most popular wireless routers used in many small and home offices. This ongoing research led to the assignment of 38 Common Vulnerabilities and Exposures (CVEs).

The research shows that 80 percent of Amazon’s top 25 best-selling SOHO wireless router models have security vulnerabilities and 34 percent of the 50 top selling models have publicly documented exploits that make it relatively simple for attackers to craft either highly targeted attacks or general attacks targeting any vulnerable systems they can find.

There is a range of protective strategies both enterprises and individuals can employ to improve SOHO wireless router security. However, a detailed survey on the adoption of these strategies shows that adoption is currently low, perpetuating a long-term risk scenario for remote workers and the enterprises who employ them.
INTRODUCTION

Where and how work gets done is changing rapidly, but the paradigms of security risk assessment are not necessarily keeping pace with these changes. The workforce is continuously moving away from tethered desktop computers protected by a wall of corporate security systems. Particularly in the technology sector, many employees expect a “work from anywhere” policy supported by employer issued laptops and personal mobile devices configured to access business data. As shown in Fig. 1, it is now quite common for employees to perform their duties from the comfort of their homes with their own Internet connections. While this shift has led to lowered costs and increased productivity, it also opens up new opportunities for cybercriminals and other malicious actors to use home networks as a gateway into otherwise well-protected enterprise infrastructures. In addition, many organizations use popular wireless routers on the corporate network and in remote offices; these are among the frequently discovered “rogue devices” that appear on corporate networks without permission of the IT department.

In order to provide more detailed insight into the scope of the security risks VERT has uncovered in SOHO routers, Tripwire partnered with Dimensional Research and OnePoll to study the use of security controls that can mitigate the risks associated with vulnerable wireless routers, both in employee home networks and in enterprises. The research includes a survey of 653 IT and security professionals and 1,009 employed consumers working remotely in either the US or the UK. Collectively, this research strongly shows a surprising number of IT professionals are not using basic security controls to harden their wireless routers. It also indicates that any corporate security policy involving remote workers is incomplete if it does not consider the risks associated with the home networks of its employees.

In an effort to understand and evaluate the security risks associated with wireless Internet access, Tripwire VERT has analyzed the security provided by the most popular wireless routers used in many small and home offices. This ongoing research, which has already led to the assignment of dozens of CVEs, makes it very clear that critical security vulnerabilities are endemic across the entire SOHO wireless router market. In fact, 74 percent of Amazon’s top 50 best-selling SOHO wireless router models have security vulnerabilities (Fig. 2). In addition, 34 percent of Amazon’s top 50 selling models have publicly documented exploits available, making it relatively simple for attackers to use this information to craft targeted attacks or simply attack all the vulnerable systems they can find. Once the attacker has gained control of a router, they are able to monitor, redirect, block or otherwise tamper with online activities. Targets that are traditionally guarded by the router’s firewall now also become targets for network-based attacks.

The goal of this white paper is to provide easily digested information on these security risks and provide mitigation advice that will allow businesses to better protect themselves from these risks.
THE SEVERITY OF SOHO ROUTER INSECURITY

Since many of the vulnerabilities discussed in this paper are still in the responsible disclosure process, vendor names and model numbers and the technical details of the vulnerabilities for specific products and exploitation techniques identified by VERT are not disclosed. Tripwire’s responsible disclosure process aims to collaborate with vendors to harden their products against the attacks identified by VERT while minimizing the potential collateral damage to consumers—an all too common side effect of premature public disclosure. Within this process, Tripwire works with vendors to confirm the vulnerability, establish reasonable timelines for patches and provides security expertise to confirm that proposed fixes are effective and complete.

In order to properly convey the severity of the security risks in many SOHO wireless routers, it’s necessary to say a few words about the type and scope of vulnerabilities that commonly exist in these products. Most of the vulnerabilities exist due to logic errors within the web-based management application used for device configuration. Virtually all models from one popular brand contain logic errors related to the web-based management system that allow an attacker to gain complete system access simply by adding a few bytes to each network request. Other brands contain a variety of authentication flaws, including some cases where a special request to the router will actually fetch the unencrypted system password.

Although many of these vulnerabilities require access to the HTTP interface, VERT has demonstrated that attackers can also make use of cross-site request forgery to exploit holes and gain access to the device by combining the vulnerabilities with social engineering techniques. Targeted attacks can also make use of locally exploitable flaws such as the well-known attacks shown in Table 1 against WEP, WPA2, and WPS. These attacks can be perpetrated by a physically proximate attacker using readily available public tools to unlock the router’s “front door.”

Once access to the configuration interface is achieved, it is essentially “game over” because many of these devices can be completely compromised with nothing more than a network connection. Most of the systems tested are also prone to memory corruption or root command injection while processing authenticated requests. Since none of the tested devices use cryptographic signatures on the firmware, an attacker can completely replace the manufacturer’s programming with a malicious version of the software. Exacerbating this risk, 30 percent of IT professionals and 46 percent of consumers do not change the admin password from its default (Fig. 3), making it even easier for attackers with access to the configuration interface to completely compromise the device.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP (Wired-Equivalent Privacy)</td>
<td>Repeated IVs can be quickly used to crack the RC4 encryption</td>
</tr>
<tr>
<td>WPA2 (Wi-Fi Protected Access II)</td>
<td>TKIP can be cracked; AES mode allows offline password cracking</td>
</tr>
<tr>
<td>WPS (Wi-Fi Protected Setup)</td>
<td>Flaws in the protocol can reveal the WPA2 passphrase</td>
</tr>
</tbody>
</table>

**TABLE 1** Well-known attacks against router encryption standards

![Default admin passwords](image_url)
Ironically, many very similar flaws were found in products from unrelated vendors, indicating that either these devices have some shared software heritage or the product developers are independently making the same mistakes. Other security vulnerabilities are not the result of programming or design errors. In fact, they are intentionally designed backdoors that are fairly easy to reverse.

Routers are an ideal target for attackers because they are commonly ignored by the user until an Internet connection fails. When they have been compromised, it can be difficult for most users to detect because they have a very minimal user interface. Even technically oriented users would likely have no idea that their router had been compromised because any traffic sent from this device to its masters would typically be “invisible” to network users using basic forensic tools. Toolkits are available to attackers that make it very easy to repackage vendor firmware to disable update functionality, and these packages conveniently include hacking tools.

Once an employee’s home router has been compromised, there are several ways an adversary can extend the compromise to gain access to corporate networks. And, businesses that use SOHO routers on their networks are at even greater risk of compromise from opportunistic attackers that convert these routers into “spies” in order to steal corporate data. Compromised SOHO routers can be used to eavesdrop on traffic sent to and from nearby enterprise access points.

Intrusion protection is rarely implemented in SOHO wireless routers, and the data flowing between the employee and the corporate network flows through them. Malicious code quietly running on the router can collect unencrypted passwords and gather data about browsing habits. Attackers using a compromised router are positioned to redirect connections with DNS hijacking and inject malicious content with man-in-the-middle (MITM) techniques that tend to be subtle and difficult for the average user to recognize.

**COMMON ATTACK VECTORS**
SOHO routers are also vulnerable to heavier-handed attacks that could render the devices useless or completely prevent user access to corporate resources. Criminal organizations could even use router vulnerabilities to carry out a “ransomware” style attack. One very real attack scenario involves compromising a router in a way that it redirects all web traffic to a malicious site which then offers to restore connectivity in exchange for payment.

While the risks from some of these attack strategies are straightforward (using routers to send SPAM, performing ad fraud and keeping lists of website visited, for example) there are two that require more description to quantify the specific risks enterprises face from successful attacks that use these strategies.

**MAN-IN-THE-MIDDLE ATTACKS**
MITM is a form of ‘active eavesdropping’ in which victims believe that they are communicating privately, but the entire conversation is controlled by the attacker. Wireless routers are an obvious target for MITM attacks.

In the case of a plain text MITM attack, the most prominent risk is malware infection. Attack code running on the router is well-positioned to insert exploits into the data moving through the router. Alternatively, an attacker can simply direct users to download malware by tampering with DNS and HTTP. Once malware has been successfully installed

![FIG. 4 Default IP addresses](image-url)
on the target system, it can be used to further compromise additional targets on the corporate network when the infected system is connected to an intranet.

Organizations using web-based SSL-VPN solutions are exposed to unique risks because an SSL MITM attack could be used directly to steal VPN credentials. Even systems that implement two-factor authentication are vulnerable because it’s possible for attack code in the router to covertly hijack access and perform actions injected into the connection by an attacker. This type of MITM attack is only partially mitigated by the use of SSL; protocol protections only work when users are conscientious about certificate warning messages, and the attacker does not have the capability to generate trusted certificates. In fact, practical attacks against SSL that rely on a combination of human and technological shortcomings are becoming more frequent every day.

The risks from passive MITM attacks are more subtle. By silently collecting data transferred through the router, the attacker can build a profile of the sites and services commonly used on the network. This information could give an attacker insight into what customers a company may be targeting, what projects it is working on, confidential legal matters, financial data, and more. For example, if an attacker observes an engineer from a particular organization is frequently accessing the website of a particular supplier, it could be inferred that this supplier is a likely candidate for an upcoming product. Similarly, having a list of websites frequented by a user can considerably increase the likelihood of a successful spear-phishing campaign.

Depending on the type of sites accessed, these exploits may also open the possibility for blackmail. In this scenario, the adversary compromises the routers of various employees that have access to information the attacker is seeking. An attacker that captures evidence of unsavory activities can then approach the victim, threatening to reveal whatever secrets were uncovered unless the victim cooperates by providing the information the attacker is seeking.

**TROJAN HORSE**

Another potential attack vector is the threat of what security researchers call a router “nuke” attack. In this scenario, an adversary attempts to infect routers with a Trojan horse designed to disable the routers at a given time or in response to control signals. Even temporarily disabling a portion of the world’s remote workforce could cost businesses millions of dollars. A more subtle denial-of-service attack would add randomized packet loss onto specific connections such as corporate VPN links, systematically degrading performance and thereby causing remote workers to be less productive. When normal websites work fine but the corporate VPN or stock trading services run slowly, victims are unlikely to identify the router as a potential source of the problem.
MITIGATION STEPS

The most effective mitigation is to remove SOHO wireless routers from enterprise and remote employee networks. Enterprises should not use SOHO routers. Businesses that rely on SOHO routers to provide network access to visitors, customers, or employees should strongly consider replacing these devices with enterprise products from vendors that build security into their products.

It should also follow that since home offices have become a de facto extension of the corporate office, it is recommended that businesses provide remote employees access points of the same quality as those used in a physical corporate office.

Since these strategies are not always viable options, VERT has identified some best practices that can be incorporated into security policies and training. If these security controls are effectively deployed, they significantly minimize the security risks from wireless router attacks.

1. Don’t enable remote management over the Internet. Embedded web servers are the source of many flaws. Corporate security policy should mandate that routers used to connect to a corporate VPN have remote management features disabled. In situations where it is necessary to manage the router remotely, it is safer to employ NAT rules allowing SSH or VPN access to manage the router. Vulnerability and configuration scanning products and services can be used to determine if employees are connecting through routers with exposed management interfaces.

2. Passwords matter. Default passwords are often the same for an entire product line or are generated from a common algorithm making a device easy prey for an attacker. It is imperative that users change passwords rather than using defaults. Use of default or weak passwords can make it possible for malicious applications or even web pages to attack the router (Fig. 3).

3. Don’t use the default IP ranges. Predictable addresses make CSRF attacks easier (Fig. 4). Rather than 192.168.1.1, consider 10.9.8.7 or something else which is not commonly used. This is a simple but effective technique for decreasing the likelihood of a successful CSRF attack.

4. Don’t forget to log out after configuring the router. Several of the routers VERT examined will not automatically log out when not in use. This can result in a situation where the web browser used to configure the router remains authenticated, opening the door for CSRF attacks. Although some CSRF attacks can be successful without authentication, this simple step will thwart traditional CSRF attacks which rely upon that authenticated browser session.

5. Turn on encryption and turn off WPS. If someone can connect to the router, it makes it much easier to attack it. Turning on AES backed WPA2 protected with a strong (26+ character) pre-shared key is ideal. WPS is a service which makes it easier for authorized clients to connect but also makes it much easier for attackers to determine your wireless passphrase, regardless of its complexity or “strength.”

6. Keep the router firmware up-to-date. Up-to-date firmware fixes known product issues, including security problems. Routinely logging into the router to check for firmware updates makes it more likely that users may notice unusual behavior that could indicate compromise (Fig. 5).
SUMMARY

The research performed by VERT demonstrates that SOHO wireless routers are plagued with vulnerabilities, many of which are not exceedingly difficult to find or to exploit. Security is not a priority for router vendors, and end users rarely consider security—as long as everything appears to work correctly. The sensitive data flowing across these devices, as well as their capability to manipulate data, makes them a prime candidate for attackers.

The results of our survey also support the possibility that attacks against wireless SOHO routers could quickly become widespread as evidenced by SANS recent discovery of “The Moon” worm currently infecting exposed Linksys routers. The risk for this kind of widespread exploit is particularly high among employed consumers who routinely connect to corporate networks from remote locations. Within this group of people, fewer than half said their router firmware was up to date, and less than a third knew how to update the firmware.

A successful attack against a wireless router provides an excellent opportunity for attackers to embed themselves into a network, making possibilities for criminal activity and espionage virtually limitless. The number of deployed routers and the relative ease of compromise make it likely that there will be an influx of malicious router infecting worms. This assertion is supported by the success of the non-malicious Carna Botnet that was used by anonymous researchers to conduct the Internet Census 2012 study. The authors of this study infected close to 1.2 million (primarily embedded) devices that had poorly chosen or default credentials. Our survey data supports the feasibility of a variety of wireless router worms because almost half of employed consumers admit they haven’t changed the administrative password on their routers. An organized campaign to compromise SOHO routers has the potential to create an enormous botnet that would not be detected by typical security controls.

The risks posed to the enterprise when employee Internet traffic can be intercepted by a compromised router are significant. Until firmware updates are available to address these security vulnerabilities, the best protection is to avoid use of routers marketed to small office and home office users. Ideally, employees should receive routers that have undergone security assessments at the same time they are issued laptops for remote use. This recommendation, in combination with a solid home network security policy, can significantly reduce the security risk to enterprise networks from wireless routers.