Enterprise Solution
Professionals on Information and Network
E-SPIN

Wireless Security Assessment and Audit Report

project

Wireless Device Vulnerability Assessment for XXXX

for

CUSTOMER NAME

date

DD MMM YYYY (Version 1.0)

prepared by

E-SPIN GROUP

Copyrighted. E-SPIN GROUP. All Right Reserved.

Our Ref: SWXX-XXXX

DD-MMM-YYYY

CUSTOMER INFO

Attn: Customer Officer, Tittle

CC: -

RE: Independent / 3rd party Wireless Security Assessment / Audit with report for XXX

We would like to express our gratitude for giving E-SPIN to provide a first service report and recommendation on reporting founding as per our subscribed service deliverables.

The report will be used as the based line for conduct "vulnerability fixing" and the second round of assessment (if subscribe) will be conduct after this to certified the status for the vulnerability whether have being fix and consider overall secured or improved.

Mr. XXX is an officer of the company who is authorised to make all commitments in this documentation and report. Future communications should be our appointed Account Manager (AM) or Customer Service Representative (CSR), once the project have being successful signed off.

Once again, it is our pleasure to assist yours on your security assessment project.

Thank you.

Yours faithfully,
for E-SPIN

Officer Name
Officer Title
Officer Department / Unit
Officer mobile mobile
Officer email

c.c. -

Copyrighted. E-SPIN Group. All Right Reserved.

Document Control

Document History

Version	Date	Author	Comments
0.9	DD MMM YYYY	Officer 1	Final Draft
1.0	DD MMM YYYY	Officer 2	Final QA Pass

Document Distribution

Version	Date	Comments
0.9	DD MMM YYYY	E-SPIN Internal
1.0	DD MMM YYYY	Release to CLIENT

Author	
Name	Officer Name
Position	Officer Title
Tel	Officer Tel
Fax	Officer Fax
Email	Officer Email
Web	www.e-spincorp.com

Copyrighted. E-SPIN Group. All Right Reserved.

Table of Contents

Item	Description	Page
1.0	EXECUTIVE SUMMARY	1
2.0	TECHNICAL DETAIL FINDINGS	5

Copyrighted. E-SPIN Group. All Right Reserved.

1.0 EXECUTIVE SUMMARY

1.1 OBJECTIVES

Understanding the vulnerabilities of your WiFi network can be challenging as users can easily create networks on demand, or even perhaps unintentionally. But as recent events have demonstrated, scanning your WiFi network is an important part of understanding your security posture.

Most vulnerability assessment tools simply take their current network scanners and point them at the wireless infrastructure. This approach does not give you the information that is unique to wireless networks. Immunity has built the first automated, WiFi specific, vulnerability assessment and penetration tool.

Copyrighted. E-SPIN Group. All Right Reserved.

1.0 EXECUTIVE SUMMARY

Unlike traditional scanners that merely identify possible vulnerabilities, SILICA determines the true risk of a particular access point. SILICA does this by unintrusively leveraging vulnerabilities and determining what assets behind the vulnerable access point can be compromised.

Additionally while traditional scanners can enumerate the vulnerabilities of a particular target, they cannot evaluate whether a mitigating control is in place on the target or in the surrounding environment. With SILICA's unique methodology it can report on whether a vulnerability can be successfully exploited.

More than simple scanning, the benefits of using SILICA include:

- Improved security posture
- Simplified trouble shooting
- Network mapping
- Create real threat profiles and vulnerability assessments
- Build WiFi risk and vulnerability analysis for PCI, SOX
- Rogue access point detection
- Auditing wireless client security

Copyrighted. E-SPIN Group. All Right Reserved.

1.0 EXECUTIVE SUMMARY

The E-SPIN team was engaged by XXX (hereinafter CLIENT) to conduct an carry in wifi security assessment on their End Client (XXX) systems to help identify any potential risks, as well as to suggest appropriate security measures to deal with any exposures uncovered, with the E-SPIN represented SILICA product solution. The intent was to see to what extent an external hacker could penetrate the systems with wifi IP, access point or controller given. This test focused on identifying technical vulnerabilities that could exploit to gain privileged access to the systems.

1.2 SCOPE

E-SPIN was engaged by CLIENT to perform wireless security assessment on the following:

- wireless network name XXX SSD XXX security XXX
- wireless network name XXX SSD XXX security XXX
- wireless network name XXX SSD XXX security XXX
- wireless network name XXX SSD XXX security XXX
- wireless network name XXX SSD XXX security XXX

For Credential Testing ID is provided as below (if any):

Admin Login
User ID: XXXXX
Password: XXXXX

Guest Login
User ID: XXXXX
Password: XXXXX

The testing was conducted over the period from Date DD-MMM-YYYY to Date DD-MMM-YYYY.

Copyrighted. E-SPIN Group. All Right Reserved.

1.3 WHAT WE TESTED FOR

A large part of the effort in performing a wireless network security assessment and audit consists of searching for information about the wireless network and looking for holes and weaknesses in the configuration or software. The team gathers as much information as they can, and use this information to search security databases for known vulnerabilities against the systems we found.

The report contains information about what was found and how it may lead to a compromise of the systems we tested. Thousands of unsuccessful automated and manual attacks have not been documented in this report, but included are areas where steps should be taken to strengthen the infrastructure to reduce the possibility of a successful attack. New exploits and vulnerabilities are being developed and discovered daily, so even though an attack may not be successful today, the same cannot be assumed about the future.

Copyrighted. E-SPIN Group. All Right Reserved.

1.4 KEY FINDINGS AND RECOMMENDATIONS

Reference	Vulnerability	Risk	Item
3.1	Fake AP (Man in the Middle)	Critical	1
3.2	Malicious Access Point Detection	Critical	1

Copyrighted. E-SPIN Group. All Right Reserved.

The risk associated with the application tested in this assessment is considered to be "Critical" - due to two(2) Critical Risk Vulnerability Item being founded.

The most critical vulnerability that the E-SPIN team came across in CLIENT wifi environment subject to Fake Access Point (Man in the middle) User ID and Password Collected due to wifi client connected to Attackers Fake AP. By using the guest ID, E-SPIN success create fake AP in the wireless network, and those who are connect to fake AP do not aware of it, and make use of the fake AP network access to various website, application and left over all the user ID and password.

If E-SPIN can collect those ID and password, so do the hacker with intent can be do so.

Another critical vulnerability detect is the Malicious Access Point Detection, it will make the wifi user easy to disclosure their ID and password without their awareness.

The E-SPIN team also found a number of less critical vulnerabilities that could be fixed to improve the security of the wifi. Based on these findings, recommended remedial actions for these vulnerabilities include:

- conduct wifi security awareness for the wifi user to educare them to be awareness for the potential risk of fake AP and malicious AP.
- If possible, isolate guess and employee access point, to avoid employee connected to the fake and malicious AP
- If possible, perform regular wireless scanning and monitoring to know in exactly what is connect in the network
- Implement some type of force SSL connection to critical application to avoid man in the middle attack
- Recommended to set strong wifi password and change frequency

E-SPIN thanks CLIENT for the opportunity to assist in your security program and look forward to working with you in the future.

Copyrighted. E-SPIN Group. All Right Reserved.

2.0 TECHNICAL DETAIL FINDINGS

2.1 INTRODUCTION

The detailed findings are contained in the following sections; each section describes the finding and includes an assessment of the risk and actions that can be taken to mitigate this risk. The findings are listed in the order in which they were discovered. This order of presentation shows how potentially low risk vulnerabilities may sometimes be used to escalate the privilege of the attacker and allow the discovery of higher risk vulnerabilities. Whilst each individual vulnerability is more or less self-contained, each of these vulnerabilities might be a stepping stone towards a full compromise of the systems. Information discovered through a single vulnerability is likely to assist the attacker in making a more serious attack later on. Therefore, it is imperative to consider all of the recommendations as a whole regardless of their apparent severity. A successful attack often requires exactly the right combination of software, ill configuration, timing and luck. Knowledge and information about a system is one of those factors. It is important to reduce the amount of information available to the attacker in order to minimize the chance of a successful attack.

2.2 VULNERABILITY LEVELS

To aid in assessing the risk associated with each vulnerability, the following risk levels are given:

Unknown	Software/system that is considered vulnerable, but the team was unable to complete testing.
Low	Information disclosure. The information gleaned from these vulnerabilities will not allow an attacker to gain direct access to systems or data. It may, however, be used to escalate a separate vulnerability.
Medium	A vulnerability that , by itself will not allow unauthorised access to systems/Data. However, two or more Medium rated vulnerabilities used in conjunction may allow an attacker unauthorised access to systems or data.
High	A medium to high level of technical knowledge is required for an attacker to gain unauthorised access to a system/data from a single vulnerability. The ability for an attacker/user to harm the professional image of a corporation.
Critical	The vulnerability could be used to comprise the application or infrastructure resulting in a severe business impact.

Copyrighted. E-SPIN Group. All Right Reserved.

3.1 Fake Access Point

Severity: Critical

Description

Impact

Potential for wifi user leftover important URL, ID and password and subject to identity theft and sensitive info lost.

Recommendation

Wifi security awareness training for employee.

Affected Item

URL, user ID and password left over by real user on the fake AP connection

Copyrighted. E-SPIN Group. All Right Reserved.

3.2 Malicious Access Point Detection
Severity: Critical

Description

Impact
Careless wifi access employee will potentially connect thru malicious access point, and unintentionally disclose sensitive information to hacker and intruder.

Recommendation
Do what is necessary to remove out those Malicious Access Point Detected from the wifi network.

Affected Item

Copyrighted. E-SPIN Group. All Right Reserved.

Supplemental Information

CLIENT XXX simplified wifi network diagram

Copyrighted. E-SPIN Group. All Right Reserved.