

**FORTCONSULT**

*Straight talk on IT security*

# ***SECURITY ADVISORY***

***March 2010***

***Intel 4965AGN wireless card information disclosure***



Discovered in May 2009 by FortConsult's Security Research Team / Warren Platt

## Table of Contents

|                                  |   |
|----------------------------------|---|
| Table of Contents .....          | 2 |
| Copyright and Disclaimer .....   | 2 |
| The Security Research Team ..... | 2 |
| Issue History .....              | 3 |
| Issue Description .....          | 4 |
| Issue Impact .....               | 4 |
| Affected Components .....        | 4 |
| Exploit .....                    | 4 |
| Mitigation .....                 | 4 |
| CVE-reference .....              | 4 |
| CVSS Base Score .....            | 4 |
| BASE SCORE: 5 .....              | 4 |

## Copyright and Disclaimer

The information in this advisory is Copyright 2010 FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

## The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team / Warren Platt.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: [www.fortconsult.net](http://www.fortconsult.net).

## Issue History

This document has been updated to the present version as information has been received from various external sources.

May 2009: Issue discovered by Warren Platt.

May 2009: Vendor notified

March 2010: Advisory publicly released

FortConsult has advised Intel Corporation's security team of the issue and they have confirmed this to be a vulnerability in June 2009. No driver updates have been released as of publishing this advisory.

## Issue Description

On booting up a machine that uses the Intel 4965AGN wireless card with the Windows Zero Configuration (WZC) supplicant enabled, probe requests to the following SSID are observed: "Intel 802.11 Default SSID".

This SSID is not present in the Preferred Network List (PNL) of the WZC supplicant.

## Issue Impact

An attacker can observe the probe request for this SSID being transmitted from the client and thereby gain knowledge of the type of wireless card used.

## Affected Components

Intel 4965AGN wireless card using HW-version 0.6.40 and Intel driver 12.2.0.11 (17.11.2008).

## Exploit

None available at the time of writing this advisory.

## Mitigation

Upgrade to the latest drivers from Intel (<http://security-center.intel.com>) when they become public.

## CVE-reference

| [CVE-2009-3285](#).

## CVSS Base Score

FortConsult has used the online CVSS calculator found at <http://nvd.nist.gov/cvss.cfm?calculator&version=2> to calculate these scores.

## BASE SCORE: 5

### Metrics:

Access Vector: Network

Access Complexity: Low

Authentication: None

Confidentiality Impact: Partial

Integrity Impact: None

Availability Impact: None