

# **[Full-disclosure] Gateway 7001 A/B/G AP: Selection of improper regulatory domains and channels**

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-11/0030.html>

---

**From:** Andrew Lockhart ([alockhart\\_at\\_networkchemistry.com](mailto:alockhart_at_networkchemistry.com))

**Date:** 11/01/05

Date: Tue, 01 Nov 2005 12:15:19 -0700

To: <bugtraq@securityfocus.com>, "full-disclosure@lists.grok.org.uk" <full-disclosure@lists.grok.org.uk>

Issue: Gateway 7001 AP allows selection of restricted 802.11a/b/g channels

Author: Network Chemistry Labs <labs at networkchemistry dot com>

Vendor: Gateway

Products: Gateway 7001 802.11 A/B/G Dual Band Wireless Access Point

Type: Input Validation

Exploit: Not required

## I. Intro

The IEEE 802.11 family of standards define the channels that a device is allowed to operate on for specific geographic regions in order to comply with different country's radio frequency usage regulations.

## II. Vulnerability

The web management interface for the Gateway 7001 A/B/G AP contains an input validation vulnerability that allows anyone authenticated with the device's built-in web server to configure the device to use channels not regulated for 802.11a/b/g use in their geographic region. The potential impact is that a user could configure the device to operate outside the allocated bandwidth for 802.11 within their country, thus causing interference to other radio systems. In addition, the device will not be visible to other 802.11 devices operating in the area.

## III. Details

The IEEE 802.11 standards provide guidance on the channels that a device may operate on in order to comply with a country's radio frequency usage regulations. As is common on many access points, the Gateway 7001 A/B/G AP provides a web based interface for configuring the device. This can be used to set the channel that the AP operates on.

The POST form in the web-management interface used to set the channel includes a form element called "RegulatoryDomain." Through experimentation it appears that this parameter affects input validation operations on the channel supplied in the request. For example, if the regulatory domain parameter is set to FCC, then the device's firmware will only change channels if the channel value in the request is from 1 to 11. Anything outside this range, such as channel 13 (a European channel), will be rejected.

However, if the regulatory domain parameter is changed, then the firmware will allow the device's channel to be changed to any channel allowed in the specified domain. This can cause the device to create interference with non-802.11 devices in the vicinity as well as allow devices to be configured to elude 802.11 security walk-throughs by operating on frequencies that the detection equipment is incapable of monitoring.

#### IV. Demonstration

In addition to POST requests, the web interface will accept the same parameters in the form of a GET request. The web-based management software for the Gateway 7001 A/B/G AP uses a request string of the following form to set configuration parameters:

<http://192.168.2.1/index.cgi?r1Mode=IEEE+802.11g&r1RegulatoryDomain=FCC&r1Channel=1&r2Mode=IEEE+802.11a&r2RegulatoryDomain=FCC&r2Channel=36&r1b1s1Ssid=NetChemLabs&r1b2s1Ssid=NetChemLabs-Guest&page=wireless.html&Update=Update>

To change the frequencies of operation available all that needs to be done is to simply change the RegulatoryDomain parameter. For instance to operate on Japanese channels, the string "FCC" would be changed to "MKK." This allows the channel parameters corresponding to the 802.11b/g and 802.11a radios to be changed to channels such as 14 and 34 respectively, which the management software will apply to the underlying hardware:

<http://192.168.2.1/index.cgi?r1Mode=IEEE+802.11g&r1RegulatoryDomain=MKK&r1Channel=14&r2Mode=IEEE+802.11a&r2RegulatoryDomain=MKK&r2Channel=34&r1b1s1Ssid=NetChemLabs+&r1b2s1Ssid=NetChemLabs-Guest&page=wireless.html&Update=Update>

It was also verified that European channels were settable when changing the RegulatoryDomain parameter to "ETSI." To verify that the device is indeed operating on non-FCC channels, special 802.11 sensor hardware was used to monitor the device on the specified channels.

The Gateway 7001 A/B/G AP makes use of DeviceScape's Instant802 Wireless Infrastructure Platform for configuration and management. It is unknown at this time whether this issue affects other devices utilizing this software, due to the fact that we have only tested

## Full-Disclosure: [Full-disclosure] Gateway 7001 A/B/G AP: Selection of improper regulatory domains and channels

the Gateway 7001 A/B/G AP at this point. Gateway also produces an 802.11 b/g version of the Gateway 7001 AP. It is also unknown whether this model is affected.

It should be noted that Gateway does not provide a firmware upgrade for the affected AP.

### V. Timeline

10/21 – Contacted Gateway: No response received  
10/21 – Contacted DeviceScape: No response received  
10/4 – Contacted Gateway: No response received  
9/28 – Contacted DeviceScape to confirm they had observed the issue: No response received  
9/26 – Contacted Gateway: No response received  
9/21 – Made contact with Gateway Support: told someone would follow-up  
9/20 – Received follow-up response from DeviceScape  
9/19 – Made contact with DeviceScape

### VI. References

Gateway 7001 A/B/G AP product support page:

<http://support.gateway.com/s/Servers/COMPO/NETWORK/7005082/7005082nv.shtml>

Instant802 WIP product page:

[http://www.devicescape.com/products/wip\\_landing.php](http://www.devicescape.com/products/wip_landing.php)

--

Andrew Lockhart <[alockhart@networkchemistry.com](mailto:alockhart@networkchemistry.com)>

Security Analyst, Network Chemistry

PGP Key ID: 58369156

Fingerprint: 0AE1 E826 1922 5453 2B34 E1AA F524 D20B 5836 9156

---

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>