802.11 Vulnerability in Clear Channel Assessment (CCA) Algorithm

Advisory Original Release Date: June 9, 2004
Last Revised: June 9, 2004
Number: 04-9
Advisory Version: 1.0

Advisory Status: Final

Overview:

The 802.11 protocol is vulnerable to an attack against the Clear Channel Assessment (CCA) algorithm used by Direct Sequence Spread Spectrum (DSSS) hardware. Non-DSSS 802.11 protocols which use either frequency hopping spread spectrum (FHSS) or orthogonal frequency division multiplexing (OFDM) are not affected by this vulnerability. These include 802.11a which uses OFDM, 802.11 which can use FHSS, and 802.11g which can use OFDM.

An attacker with access to a wireless network can cause other nodes within range to believe that the channel is not clear to send, effectively causing a denial of service. This vulnerability is in the standard algorithm thereby affecting all Avaya 802.11g and 802.11b devices using DSSS. However, there are geographical limits to the attack (approximately 50 feet).

More information about this vulnerability can be found in the security advisory issued by AusCERT and in CERT vulnerability note 106678.

Recommended Actions:

Consider security and availability requirements carefully when deciding to use wireless networks for sensitive/critical applications.

Avaya will track the standards as a resolution is designed. Until a complete solution is made available Avaya recommends the use of 802.11a or 802.11g utilizing OFDM which is not affected by this vulnerability. All Avaya Wireless Access Points support 802.11g, some via upgrade kits.

The following Avaya hardware products run on 802.11 and may be vulnerable.

System Products

Product	802.11 Variant Supported
Avaya Wireless AP-3	Supports 802.11a. Upgrade kit available for 802.11g support.
Avaya Wireless AP-4	Supports 802.11b. Upgrade kit available for 802.11 (abg) supports.
Avaya Wireless AP-5	Supports 802.11a. Upgrade kit available for 802.11 (abg)

	supports.
Avaya Wireless AP-6	Supports 802.11g
Avaya Wireless AP-8	Supports 802.11 (abg)

Additional Information: Additional information may also be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-866-GO-AVAYA, with any questions.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.