Static WEP Key Vulnerability Disclosure

Advisory Original Release Date: December 15, 2005
Last Revised: December 15, 2005
Number: ASA-2005-233
Risk Level: High
Advisory Version: 1.0

Advisory Status: Final

Overview:

Avaya Wireless Access Points (AP) provide authentication and access to network resources via IEEE 802.11a, 802.11b and 802.11g.

Urmas Kahar and Tarmo Kaljumäe have reported a static WEP Key vulnerability in the Avaya Wireless AP product line. A static WEP key of "12345" can be used to bypass 802.1x authentication, and gain access to available network resources. This issue affects the Avaya Wireless AP-3, AP-4, AP-5, AP-6, AP-7, and AP-8. The Common Vulnerability and Exposures project (cve.mitre.org) has assigned the name CVE-2005-3253 to this issue.

The Avaya Wireless Access Points are manufactured by Proxim Wireless, and this vulnerability has also been addressed by Proxim Wireless at:

AP-2000

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1221

AP-600:

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1222

AP-700:

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1686

AP-4000:

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1250

Mitigating Factors:

Only certain firmware levels are affected by this issue. For Avaya Wireless AP 3-6 only firmware 2.5 to 2.5.4 are affected. For Avaya Wireless AP-7 and 8 only

Affected System Products

Product	Affected S/W Version	Comments and Recommended Actions	Risk Level
Avaya™ Wireless Access Points AP-3, AP-4, AP-5, and AP-6	All Versions after 2.5 to 2.5.4	Avaya Wireless AP firmware 2.5.5 has been released to address this vulnerability. Follow All users should apply version 2.5.5 (or later) to address this vulnerability. See Recommended Actions below.	High
Avaya™ Wireless Access Points AP-7 and AP-8	All Versions after 2.5 and prior to 3.1	Avaya Wireless AP firmware 3.1 has been released to address this vulnerability. All users should apply version 3.1 (or later) to address this vulnerability (see below for more information).	High

Recommended Actions:

Avaya Wireless AP-3

Download and install Software Update 2.5.5 for AP3 -

http://support.avaya.com/japple/css/japple?temp.documentID=280939&temp.productID=107770&temp.bucketID=108025&PAGE=Document

Avaya Wireless AP-4, 5, and 6:

Download and install Software Update 2.5.5 for AP4, 5 and 6 -

http://support.avaya.com/japple/css/japple?temp.documentID=280948&temp.productID=107770&temp.bucketID=108025&PAGE=Document

Avaya Wireless AP-7:

Download and install Software Update 3.1 for AP7 -

http://support.avaya.com/japple/css/japple?temp.documentID=280946&temp.productID=107770&temp.bucketID=108025&PAGE=Document

Avaya Wireless AP-8:

Download and install Software Update 2.5.5 for AP4, 5 and 6 -

http://support.avaya.com/japple/css/japple?temp.documentID=280948&temp.productID=107770&temp.bucketID=108025&PAGE=Document

Special Acknowledgements:

Avaya thanks and credits Tarmo Kaljumäe and Urmas Kahar for bringing this issue to our attention as well as working with Avaya to help protect our customers.

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 1-800-242-2121, 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.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

Revision History:

V 1.0 - December 15, 2005 - Initial statement issued.

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