

Cisco Security Response: Cisco Response to TKIP Encryption Weakness

<http://www.cisco.com/warp/public/707/cisco-sr-20081121-wpa.shtml>

Revision 1.0

For Public Release 2008 November 21 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Cisco Response](#)
[Additional Information](#)
[Status of this Notice: FINAL](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

Several technology trade and other press outlets have recently released stories about security vulnerabilities in the Temporal Key Integrity Protocol (TKIP). TKIP was developed after security vulnerabilities were found in the Wired Equivalency Protocol (WEP). This protocol was developed as a stopgap mechanism to address wireless security limitations in WEP for wireless devices that could not support the Advanced Encryption Standard (AES).

TKIP is the mandatory cipher suite for the first version of the Wi-Fi Protected Access (WPA) specification and it is an option for the Wi-Fi Protected Access version 2 (WPA2) standard.

Additional Information

A weakness exists in TKIP that can allow an attacker to decrypt packets under certain circumstances. This is not a key recovery attack. The attacker can only recover the key used to authenticate packets but not the key used to encrypt and obfuscate data. With the recovered key, only captured packets may be forged in a limited window of at most 7 attempts. The attacker can only decrypt one packet at a time,

currently at a rate of one packet per 12-15 minutes. Additionally, packets can only be decrypted when sent from the wireless access point (AP) to the client (unidirectional). Only devices configured to use TKIP as the encryption mechanism are affected by these attacks. Customers who use WPA2 with the AES-CCMP cipher suite are not vulnerable to these attacks.

AES is a more secure encryption algorithm and has been deemed acceptable for the US government to encrypt both non-classified and classified data. At this time, there are no known successful attacks to break an AES encryption key. AES is the current highest standard for encryption, and replaces WEP; therefore, the use of WPA2 with AES is recommended whenever possible. Its predecessor, WPA, was an interim protocol. The majority of recent wireless devices and clients support the AES encryption standard.

Note: For a list of WPA2-supported clients, please visit <http://www.wi-fi.org>

If a client does not support WPA2 with AES due to age of the hardware or lack of driver compatibility, a VPN is the next best solution for securing over-the-air client connections. A VPN combined with network segmentation using multiple SSIDs and VLANs provides a robust solution for networks with varied clients. IP Security (IPSec) and Secure Sockets Layer (SSL) VPNs provide a similar level of security as WPA2.

The following workarounds and mitigations are available when WPA2 with AES is not available.

Workarounds and Mitigations

To mitigate this issue, users are advised to rotate the pairwise key more frequently. While it has been suggested that 120 seconds be the rekey interval, using a rotation interval of 300 seconds should be sufficient in most environments as the attacker must take on the order of 8 minutes or longer to recover the partial key, a longer interval may still be adequate and would result in less of a load on the RADIUS server.



Caution: Decreasing the key rotation interval will increase the load on the RADIUS server if using EAP.

On Autonomous APs the **dot1x timeout reauth-period** *<nSeconds>* command can be used to modify the key rotation interval.

Note: This command can be used globally per AP; per wireless domain services (WDS); or as provided from a RADIUS server, depending on the configuration.

On the Wireless LAN Controller (WLC) web console navigate to **WLANs > Advanced > Enable Session Timeout**. Alternatively, the **config wlan session-timeout** *<wlanID>* *<nSeconds>* command line interface (CLI) command can be used to modify the key rotation interval.

Disabling WMM is still being investigated as a viable workaround on Cisco products.

Message Integrity Check (MIC) errors incorporated in Wi-Fi Protected Access (WPA) are not necessarily indicative of an attack; in fact, various clients, such as Cisco 7920 phones, are known to occasionally generate MIC errors in normal operation. However, a carefully executed instance of this attack will generate MIC errors at a rate of less than once per minute, to prevent triggering AP

countermeasures. The following is an example of the Wireless LAN Controller (WLC) system message seen when AP countermeasures have been activated:

```
The AP '00:0b:85:67:6b:b0' received a WPA MIC
error on protocol '1' from Station '00:13:02:8d:f6:41'.
Counter measures have been activated and traffic has
been suspended for 60 seconds.
```

This error may indicate that someone in the network is attempting to replay the message that was sent by the original client, or that the client is faulty. If a client repeatedly fails the MIC check, the controller disables that WLAN for 60 seconds as per the WPA protocol requirements. This prevents a possible attack on the encryption scheme. These MIC errors cannot be turned off on the controllers. For more information refer to the Wireless LAN Controller (WLC) Error and System Messages FAQ at the following link:

http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008082c464.shtml

Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Revision History

Revision 1.0	2008-November-21	Initial public release.
--------------	------------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

-

Please rate this document.

-

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)