



ICASI Advisory

Wi-Fi Protected Access (WPA) Encryption Vulnerability

Situation

ICASI is aware of reports in early November of 2008 that describe a way to partially crack the Wi-Fi Protected Access (WPA) encryption standard used to protect data on many wireless networks. The documented issue affects encryption solutions that implement WPA-TKIP and allows an attacker to inject network traffic between an Access Point and a Client if multimedia extensions are used. Encryption solutions that implement Advanced Encryption Standard (AES) are not affected by this issue.

This issue confirms that security of wireless devices and wireless network traffic remains a topic of interest for security researchers and should be high on the agenda of all companies.

ICASI believes this issue poses a moderate risk.

ICASI Recommendation

ICASI recommends that companies switch to WPA2 with AES-CCMP and that future implementation decisions include hardware support for strong encryption. For more information on how to make the switch, please consult your wireless hardware vendor's documentation and/or Web site.

For More Information

Please see the following for attack details:

<http://dl.aircrack-ng.org/breakingwepandwpa.pdf>

Please note that a tool was written and distributed to implement this attack. Please see the following URL for specific information:

<http://www.aircrack-ng.org/doku.php?id=tkiptun-ng>

Additionally, please note that Aircrack can also be updated with this functionality through the Subversion (SVN) version control system.

Today, all newer wireless hardware should support AES-CCMP. However, when AES was initially implemented, some hardware had insufficient capability to support AES encryption. The WPA-TKIP was an interim solution developed to fix the key reuse problem of Wired Equivalence Privacy (WEP), providing a transition mechanism from WEP until all hardware supported AES-CCMP encryption. For nearly five years, WPA-TKIP worked without issues. Now that security researchers have partially cracked WPA-TKIP, it is likely that further evolution in the attacks against WPA-TKIP will continue.

Feedback

Please address any comments regarding this advisory to: industrynotices@icasi.org.

