

[NEWS] Car Whisperer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0025.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/07/05

To: list@securiteam.com

Date: 7 Aug 2005 17:28:21 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Car Whisperer

SUMMARY

The carwhisperer project intends to educate manufacturers of carkits and other Bluetooth appliances to the possibility of a security threat caused by the use of standard passkeys.

DETAILS

A Bluetooth passkey is used within the pairing process that takes place, when two Bluetooth enabled devices connect for the first time. Besides other public data, the passkey is a secret parameter used in the process that generates and exchanges the so-called link key. In Bluetooth communication scenarios the link key is used for authentication and encryption of the information that is exchanged between the counterparts of the communication.

The cw_scanner script repeatedly performs a device inquiry for visible Bluetooth devices of which the class matches the one of Bluetooth Headsets and Hands-Free Units. Once a visible Bluetooth device is found and it has the appropriate device class is found, the cw_scanner script executes the carwhisperer binary that connects to the found device (on RFCOMM channel 1) and opens a control connection and connects the SCO links.

Securiteam: [NEWS] Car Whisperer

The carwhisperer binary connects to the device found by the cw_scanner. The passkey that is required for the initial connection to the device is provided by the cw_pin.pl script that replaces the official BlueZ PIN helper (graphical application that usually prompts for the passkey). The cw_pin.pl script provides the passkey depending on the Bluetooth address that requests it. Depending on the first three bytes of the address, which references the manufacturer, different passkeys are returned by the cw_pin.sh script. In quite a few cases the preset standard passkey on headsets and handsfree units is '0000' or '1234'.

Once the connection has been successfully established, the carwhisperer binary starts sending audio to, and recording audio from the headset. This allows attackers to inject audio data into the car. This could be fake traffic announcements or nice words. Attackers are also able to eavesdrop conversations among people sitting in the car.

Ideally, the carwhisperer is used with a toooned dongle and a directional antenna that enhances the range of a Bluetooth radio quite a bit. (see Long-Distance-Snarf experiment)

Recommendations:

In order to avoid getting attacked by carwhisperer, manufacturers should not use standard passkeys in their Bluetooth appliances. Moreover, there should be some kind of direct interaction with the device that allows a device to connect. Another recommendation would be to switch the handsfree unit to invisible mode, when no authorized device connects to it within a certain time.

Not all Bluetooth carkits are subject to this threat. There is quite a few Bluetooth carkits that use random passkeys that are generated for every individual device during the production process. Carkits that are integrated with a full infotainment system could use (and sometimes already do use) the infotainment system's UI for acquiring a passkey from the user.

Proof of Concept:

A proof of concept can be found at:

<http://trifinite.org/Downloads/carwhisperer-0.1.tar.gz>

<http://trifinite.org/Downloads/carwhisperer-0.1.tar.gz>

ADDITIONAL INFORMATION

The information has been provided by <mailto:juha-matti.laurio@netti.fi> Juha-Matti Laurio .

The review was written by <mailto:martin@trifinite.org> Martin Herfurt.

The original article can be found at:

http://trifinite.org/trifinite_stuff_carwhisperer.html

http://trifinite.org/trifinite_stuff_carwhisperer.html

=====

Securiteam: [NEWS] Car Whisperer

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.