

[Full-disclosure] WEP-Client-Communication-Dumbdown (WCCD) Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-01/msg00528.html>

- *From:* security@xxxxxxxxxxxxxxxxxx
 - *Date:* Mon, 16 Jan 2006 17:23:06 +0800
-

ThinkSECURE Pte Ltd (www.securitystartshere.net) has released details of a client-side wireless vulnerability which affects wireless users who are still using WEP.

More details including mitigation actions are available at our website at:

<http://www.securitystartshere.net/page-vulns-wccd.htm>

Vulnerability Name

WEP-Client-Communication-Dumbdown (WCCD) Vulnerability

Vulnerability Description

ThinkSECURE has discovered that certain well-known wireless chipsets, using vulnerable drivers under the Windows XP operating system and when configured to use WEP with Open Authentication, can be tricked by a 802.11-based wireless client adapter operating in master mode ("the attacker") to discard the WEP settings and negotiate a post-association connection with the attacker in the clear.

We have named this vulnerability as the "WEP-client-communication-dumbdown" (wccd) vulnerability.

This vulnerability is apparently not due to Windows itself but due to the operation of the drivers for the affected wireless cards.

However, this does not discount a situation where a patch could be released by Microsoft to deal with the problem on the chipset makers' behalf.

Again, this is apparently NOT a Windows problem but a wireless chipset driver-related one.

End-users of the system would not notice any difference about the clear connection that was being established.

[Full-disclosure] WEP-Client-Communication-Dumbdown (WCCD) Vulnerability

Although WPA/2 & WPA-PSK have been out for some time now, in our experience there is still a large installed client base who are still using WEP-enabled Access Points and thus have WEP-enabled profiles setup in their laptops. This installed base is vulnerable.

Vulnerability Impact

The vulnerability was observed in a Windows XP wireless client configuration with the vulnerable drivers and with the following setups:

1. Profile configured using Windows XP zero configuration as well as using the vulnerable drivers' bundled wireless client managers;
2. Profile configured to use WEP with static WEP key & Open Authentication.

Using ThinkSECURE's recently-released security auditor's tool – probemapper – one can remotely evaluate the SSID and capabilities of wireless profiles from probe requests and assess whether the subject is probing for any Open-Authentication-WEP-encryption-enabled wireless networks.

When a Windows XP client using a vulnerable chipset driver is configured as outlined above via their wireless profiles ("the victim"), the victim will send out probe requests bearing the SSID configured in the wireless profile.

An attacker who detects the probe request frames coming from the configured profile can configure a master-mode-enabled wireless card with the detected SSID of the probe request frames and, using Open Authentication with no-encryption, send probe responses to the victim.

The victim will then initiate authentication and association, sending an association request frame with the Privacy Bit set to 1 (AP/STA can support WEP).

The attacker returns an association response frame with Privacy Bit set to 0 (AP/STA cannot support WEP).

Although the correct behavior should be to not establish any communication due to the difference between association request and response Privacy Bits, the victim "dumbs-down" and establishes an un-encrypted communications session to match the attacker's Privacy Bit setting of 0, thus ignoring the WEP settings as configured in the client's profile. All traffic to & from this connection will be sent in the clear.

A victim who has a vulnerable wireless network at home and brings a laptop bearing the profile of said home wireless network to his/her organization and plugs in using a wired connection may be attacked in this manner and used as a conduit by the attacker, through the

bridging of the laptop's wireless interface to the wired interface, to the victim's organization's wired network, thus bypassing corporate perimeter defences. It is irrelevant that the organization does not use wireless or has a no-wireless policy if that policy is not strictly enforced through proactive checking.

Also, firewalling on the victim's laptop might not guarantee safety in certain cases: e.g. the attacker issues an IP address and gateway address to the victim in response to the victim's typical DHCP request upon association so as to fool the victim's machine into forwarding all traffic to the attacker's machine. The result is that, when the victim opens up a web browser for example, he will see a crafted page bearing malicious code on the attacker's machine which runs exploit code on the victim's machine (a good example being the recent WMF vulnerability) to give the attacker a reverse shell into the victim, where the attacker can then do the bridging of the interface or anything else he wants.

Vulnerability Cause

In our testing, we have narrowed down the cause of the problem to stem from the way certain chipset manufacturer drivers deployed for the Windows platform operate in handling an association.

Affected chipset manufacturer(s) have been notified via their website contact addresses.

In the interests of responsible disclosure, we will not be stating which chipset drivers which we tested as vulnerable for a minimum period of 14 days after this vulnerability advisory, thus giving time for the notified vendors to issue non-vulnerable drivers. (dated 16 Jan 2006)

Vulnerability Discovery Acknowledgment

Christopher Low & Julian Ho of ThinkSECURE Pte Ltd (<http://www.securitystartshere.net>) discovered and researched this vulnerability from Dec 2005 to 15 Jan 2006."

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

- Prev by Date: [\[Full-disclosure\] \[SECURITY\] \[DSA 942-1\] New albatross packages fix arbitrary code execution](#)
- Next by Date: [\[Full-disclosure\] Virata-EmWeb DSL modems](#)

[Full-disclosure] WEP-Client-Communication-Dumbdown (WCCD) Vulnerability

- Previous by thread: [*\[Full-disclosure\] \[SECURITY\] \[DSA 942-1\] New albatross packages fix arbitrary code execution*](#)
- Next by thread: [*\[Full-disclosure\] Virata-EmWeb DSL modems*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)