

[NEWS] KisMAC Cisco Vendor Tag Encapsulated SSID Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00086.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 27 Mar 2006 19:21:38 +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>

KisMAC Cisco Vendor Tag Encapsulated SSID Overflow

SUMMARY

<<http://www.kismac.de>> KisMAC is "a free stumbler application for MacOS X, that puts your card into the monitor mode. Unlike most other applications for OS X it has the ability to run completely invisible and send no probe requests."

While Stefan played around with wifi, raw packets, MacOS X, ppc and KisMAC a quick audit revealed a remotely triggerable buffer overflow in KisMAC's parser for tagged data in 80211 management frames, that can lead to execution of arbitrary code.

To exploit this vulnerability an attacker must either trick the victim in opening a pcap file containing the special crafted management frames OR the attacker must send such raw frames while the victim is performing a passive network scan.

DETAILS

Vulnerable Systems:

- * KisMAC dev version 113 and prior

[NEWS] KisMAC Cisco Vendor Tag Encapsulated SSID Overflow

* KisMAC version 73p and prior

Immune Systems:

* KisMAC dev version 114 or newer

* KisMAC version 74p or newer

When KisMAC receives a 80211 management frame (or finds one in a imported pcap file) it parses the attached tagged data with the function WavePacket:parseTaggedData. With the help of this method the SSID, the channel and the rates get extracted from the management packet.

The function in question also supports a special Cisco vendor tag, which is scanned by KisMAC for additional SSIDs. Unfortunately it then copies the SSIDs found into a 33 bytes big stackbuffer without any kind of size check.

```
slen = (*(ssidl + 5)); // <-- reading SSID length (UINT8)
ssidl += 6;

if ((len -= slen) < 0) break;

@try {
memcpy(ssid, ssidl, slen); // <-- copying without check into 33
// bytes big stackbuffer
ssid[slen]=0;
[_SSIDs addObject:[NSString stringWithUTF8String:ssid]];
}
@catch (NSEException *exception) {
[_SSIDs addObject:[NSString stringWithCString:(char*)(ssidl)
length:slen]];
}
```

Due to the try/catch block around the memcpy() the stacklayout allows to overwrite the jump_buf for setjmp/longjump which are used for the exception handling. This actually means it is not only possible to control the execution flow by manipulating the program counter (pc) but also to have control over the content of all registers once the execution flow has been manipulated.

It should be obvious that this eventually leads to the execution of arbitrary code.

Disclosure Timeline:

- 22. March 2006 – Contacted KisMAC developers by email
- 22. March 2006 – Vendor releases KisMAC update
- 23. March 2006 – Public Disclosure

ADDITIONAL INFORMATION

[NEWS] KisMAC Cisco Vendor Tag Encapsulated SSID Overflow

The information has been provided by <<mailto:sesser@xxxxxxxxxxxxxxxxxx>>
Stefan Esser.

The original article can be found at:
<http://www.hardened-php.net/advisory_032006.115.html>
http://www.hardened-php.net/advisory_032006.115.html

=====

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@xxxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxxx

=====
=====

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.