Subject: router wi-fi a rischio intrusione
Posted by mario on Sun, 09 Jan 2011 07:38:16 GMT
View Forum Message <> Reply to Message

alcuni pirati informatici hanno trovato il modo di rendere vulnerabili
le password di alcuni router di reti wi-fi domestiche particolarmente
diffusi che vengono dati in comodato da alcuni provider.Nell'articolo
non Ã¨ specificato se il problema interessa anche gli utenti linux

http://snipurl.com/1szcl9
saluti mario

Subject: Re: router wi-fi a rischio intrusione
Posted by Cinuda on Sun, 09 Jan 2011 11:36:54 GMT
View Forum Message <> Reply to Message

Il 09/01/2011 08:38, mario ha scritto:
> alcuni pirati informatici hanno trovato il modo di rendere vulnerabili
> le password di alcuni router di reti wi-fi domestiche particolarmente
> diffusi che vengono dati in comodato da alcuni provider.Nell'articolo
> non Ã¨ specificato se il problema interessa anche gli utenti linux
>
> http://snipurl.com/1szcl9
> saluti mario

Era un problema dei router dati in comodato da Alice. Fino a poco tempo
fa non si poteva cambiare la password di default e, di conseguenza era
stato trovato un sistema che, mi pare in base all'essid, ricavava la
password dei router suddetti. Ora, con gli ultimi aggiornamenti che la
Telecom ha fatto in automatico ai suoi router, e' possibile cambiare la
password per il collegamento wi-fi. La stessa Telecom, nell'ultima
bolletta, consiglia di cambiare la password e mette un indirizzo web per
le istruzioni. Io da un pezzo ho cambiato router :)

--
Ciao, Stefano.

La giovinezza sarebbe un periodo piÃ¹ bello se solo arrivasse un po' piÃ¹
tardi nella vita. (Charlie Chaplin)

Subject: Re: router wi-fi a rischio intrusione
Posted by archiunix on Sun, 09 Jan 2011 11:45:41 GMT
View Forum Message <> Reply to Message

Il 09/01/2011 08:38, mario ha scritto:

> alcuni pirati informatici hanno trovato il modo di rendere vulnerabili
> le password di alcuni router di reti wi-fi domestiche particolarmente
> diffusi che vengono dati in comodato da alcuni provider.Nell'articolo
> non Ã¨ specificato se il problema interessa anche gli utenti linux
>
> http://snipurl.com/1szcl9
> saluti mario

Il problema interessa tutti gli utenti in possesso di un router wi-fi
che non permette di modificare la password di default.
Il sistema operativo usato non c'entra nulla.
Ciao
--
  ."`.   ~Archimede~
: :' : *Powered by GNU/Linux Debian-SID*
`. `'`   Kernel 2.6.36-i686 & Gnome 2.30
   `-   Linux Registered User #321566

Subject: Re: router wi-fi a rischio intrusione
Posted by Lem Novantotto on Sun, 09 Jan 2011 12:45:38 GMT
View Forum Message <> Reply to Message

Cinuda ha scritto:

> Era un problema dei router dati in comodato da Alice.

Comunque Ã¨ vero che il semplice WPA Ã¨ da circa un anno un'alternativa non
piÃ¹ cosÃ¬ sicura come si credeva. In *certe* situazioni, il traffico verso il
client risulta integralmente decrittabile:
 http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip _michael.pdf.

Per non saper nÃ© leggere nÃ© scrivere, WPA2 e vivere felici.
Per ora, almeno. ;)

BTW: i sistemi operativi delle macchine coinvolte nella rete *sono*
rilevanti. Non banalmente, non per gli attacchi classici. Ma per attacchi
sofisticati come quelli descritti in nota, sÃ¬. Cito, per esempio:

[...]
However, many Linux systems send a zero ID within the IP header of TCP-RST
packets and many wireless access points are running linux, so in that case an attacker
gains the two extra keystream bytes from listening to TCP-RST packets, followed by
the flags and fragment field. As there are no other fragments, this is always zero and
the flags would be either 0x40 for a â€œdonâ€™t fragmentâ€• flag set, or zero otherwise. The
next â€œTTLâ€• field is often set to 0x40 as a default by linux systems and the protocol
on top of IP will be TCP, as we specified that, which gives a 0x06 on that byte.
The source and destination IPs are also known, as we chose them initially, so the IP

header checksum can be calculated and inserted.Now we got the complete IP header keystream. The TCP header is also completely known to the attacker, as the ports were chosen in the first place, the sequence number will be the same as the original incremented by one and the ack number will be zero. Header length and flags are always set to 0x50 and 0x04 describing a 20 bytes TCP header and the RST flag being set. The window- and urgent field will be zero in TCP-RST frames and the Checksum can again be computed as all necessary fields are known.
So in case the attacker finds the IP of a local linux system, which has the described features, the complete TCP-RST packet can be guessed, including the MIC and ICV bytes, which generates a new (8 bytes LLC, 20 bytes IP, 20 bytes TCP, 8 bytes MIC and 4 bytes ICV) 60 bytes keystream, which in return can be used alone to encrypt a TCP-SYN packet, that generates up to 7 new 60 bytes keystreams without any fragmentation needed.
[...]
--
Bye, Lem
Ceterum censeo ISLAM esse delendum

_____ _____
Non sprecare i cicli idle della tua CPU. Usali per qualcosa di utile.
http://orbit.psi.edu/ http://www.worldcommunitygrid.org/index.jsp
http://boinc.berkeley.edu/projects.php

Subject: Re: router wi-fi a rischio intrusione
Posted by daniele on Mon, 10 Jan 2011 08:26:42 GMT
View Forum Message <> Reply to Message

Lem Novantotto <Lem98@Hotmail.com> writes:

> Btw: i sistemi operativi delle macchine coinvolte nella rete *sono*
> rilevanti. Non banalmente, non per gli attacchi classici. Ma per attacchi
> sofisticati come quelli descritti in nota, sÃ¬. Cito, per esempio:

AltrochÃ©, se non sbaglio in XP Ã¨ possibile recuperare la chiave WAP dal registro di sistema.
--
Dona i tuoi cicli di clock alla ricerca!
http://boinc.berkeley.edu/

Chi ama irrita sempre chi non ama.
