**F-Secure har upptäckt ännu en sårbarhet i en router för konsumentmarknaden**

*Säkerhetsluckan öppnar upp hemmets internettrafik – ännu ett bevis på vilket stort problem svag säkerhet i routrar är*

Helsingfors, Finland, 2 september, 2016: Säkerhetsforskare på F-Secure har upptäckt en kritisk sårbarhet i en del routermodeller från tillverkaren Inteno som, om den utnyttjas, är så allvarlig att den ger personen bakom attacken full tillgång till enheten och den trafik som passerar genom den.

Sårbarheten gör det möjligt för dem att installera ett eget firmware på enheten, en ny systemmjukvara som skulle fungera och se ut precis som tidigare – men som innehåller bakdörrar och en uppsjö ovälkomna tillskott i funktionsväg. Genom att utnyttja säkerhetsluckan går det till exempel att tjuvlyssna på all trafik som inte är krypterad, inte bara trafik till och från internet utan även trafik mellan enheter på nätverket. En annan möjlighet är att personerna bakom attacken kapar surfsessionerna och skickar användaren till skadliga sajter preparerade med trojaner och liknande.

”Genom att byta firmware kan personen bakom attacken ändra vilken inställning eller regel som helst på routern”, säger Janne Kauhanen, cybersäkerhetsexpert på F-Secure. ”Tittar du på en film som ligger på en annan dator? Det gör personen bakom attacken också. Uppdaterar du en annan enhet uppkopplad via routern? Det är bara att hoppas att det inte finns några liknande sårbarheter på den. Den trafik som går över https är krypterad, så den är inte lika enkel att spionera på. Men de kan fortfarande styra om all trafik till skadliga sajter som planterar trojaner och andra elakheter på din dator.”

Routertypen i fråga tar vanligtvis emot uppdateringar av firmware från en server som drivs av användarens internetoperatör. Problemet är att de inte gör något för att säkerställa att det är rätt uppdatering, att den är okej och att den kommer från rätt plats. En cyberbrottsling som redan har tillgång till trafiken mellan routern och operatörens uppdateringsserver (till exempel genom att få tillgång till anslutningspunkten i ett flerfamiljshus) kan enkelt sätta upp sin egen uppdateringsserver och låta den distribuera en skadlig variant av uppdateringen.

Enligt F-Secures forskarlag är det här fallet bara toppen av isberget när det handlar om routersäkerhet. Det är ett problem som blir än större tack vare att så få är medvetna om att det existerar – de flesta konsumenter är helt ovetande om att det finns sårbarheter i deras routrar.

”Det är löjeväckande att det finns enheter på marknaden som är så här sårbara”, säger Janne Kauhanen. ”Vi och andra säkerhetsföretag hittar sårbarheter i den här typen av enheter hela tiden. Firmware på routrar och olika typer av IoT-enheter är bortglömda av såväl tillverkarna som deras kunder, av alla egentligen – utom av brottslingarna, som utnyttjar sårbarheterna till att kapa internettrafik, stjäla information och sprida skadlig kod.”

Även om den aktuella säkerhetsluckan är allvarlig så är det inte helt trivialt att exploatera den. Den som vill sjösätta en attack behöver befinna sig inne i nätverket, någonstans mellan routern och anslutningen mot internet.

De routrar som F-Secure konstaterat är påverkade av säkerhetsluckan är Inteno-modellerna EG500, FG101 och DG201 – men företaget har inte undersökt alla routrar och det är möjligt att fler har samma problem.

Detta är en typ av routrar som ofta distribueras av internetoperatörer, som en del av sina abonnemangslösningar.

Enligt Harry Sintonen, den säkerhetskonsult som upptäckte sårbarheten, finns det inget sätt för konsumenterna att förhindra att deras router utnyttjas – bortsett från att byta ut den mot en modell som inte är sårbar – eller att se till att uppdatera till en firmware-version som åtgärdar problemet så fort det finns en sådan tillgänglig.

Men han påpekar också att det är problematiskt att uppmana till att byta ut routern. ”Sårbarheter är så pass vanligt bland den här typen av utrustning att det är möjligt att bytet bara resulterar i att säkerhetsläget blir ännu sämre.”

Men det går att riskminimera genom att följa några ganska enkla säkerhetsråd:

* Håll operativsystem, webbläsare och annan mjukvara uppdaterade för att göra det svårare för personen bakom attacken att orsaka ytterligare skada.
* Använd en [pålitlig säkerhetslösning](https://www.f-secure.com/en_US/web/home_us/safe) som håller sig uppdaterad för att förhindra att det planteras skadlig kod på maskinen.
* Använd en [VPN-lösning](https://www.f-secure.com/en_US/web/home_us/freedome) för att kryptera all internettrafik. Även om routern blir utsatt så skulle det förhindra personen bakom attacken från att spionera.
* Kör [F-Secure Router Checker](https://campaigns.f-secure.com/router-checker/en_global/) för att vara säker på att din router inte ansluter till skadliga DNS-servrar.

F-Secure har beskrivit säkerhetsluckan för såväl myndigheter som tillverkare innan den offentliggjordes.

**För mer information vänligen kontakta:**Gia Forsman-Härkönen, PR Manager, Nordics
+358 50 324 30 78
gia.forsman-harkonen@f-secure.com

**Switch on Freedom!**
F-Secure har försvarat miljontals människor runt om i världen från digitala hot i över 25 år. Våra prisbelönta produkter skyddar människor och företag mot allt från skadliga program till cyberattacker mot företag, och är tillgängliga genom över 6000 återförsäljare och 200 operatörer i mer än 40 länder. Vårt uppdrag är att hjälpa människor att säkert koppla ihop sig med världen, so join the movement and switch on freedom!

Grundat 1988. F-Secure är noterat på NASDAQ OMX Helsinki Oy

[*f-secure.com*](http://www.f-secure.com/)|[*twitter.com/FSecureSWE*](http://www.twitter.com/FSecureSWE)|[*facebook.com/f-secure*](http://www.facebook.com/f-secure)