HTTP.sys – remote code execution i smiješno jednostavan DoS

Nedavno otkrivena ranjivost u upravljačkom programu HTTP.sys ostavlja mnoge verzije Windowsa ranjivima na *remote-execution* napad. Iako su prvi izvještaji govorili o ranjivosti IIS-a, odnosno Microsoftovog web servera, ranjivost je primjenjiva na cijeli spektar verzija Windowsa i aplikacija: HTTP.sys je upravljački program koji se izvršava u prostoru kernela i to napad čini izuzetno opasnim, jer uspješno izveden daje napadačkom kodu najviše privilegije.

Zbog toga nisu ranjivi samo IIS 6.0 i viši, već i desktopi: Windows 7 i noviji, sa bilo kojom aplikacijom koja koristi navedeni upravljački program, te naravno Windows server 2008 R2 i noviji.

Napad koristi ranjivost u kodu koji obrađuje specifičan parametar HTTP zahtjeva: "range" polje u zaglavlju koje se koristi za dohvaćanje dijela informacije (datoteke) sa poslužitelja, a čijom manipulacijom napadač može navesti IIS (te svaku drugu aplikaciju koja koristi HTTP.sys) na izvršenje u zahtjev ubačenog koda. Taj će se kod zatim izvršiti pod ovlastima koje ima HTTP.sys, koji je – oh, nesreće – ni više ni manje već kernel mode device driver.

Kako na svojoj stranici [1] navodi Mattias Geniar, ovu ranjivost moguće je iskoristiti i za iznimno efikasan DoS napad, jer ranjivi poslužitelj poplavi već nakon dva pažljivo sročena HTTP zahtjeva.

Mattias također nudi i vrlo jednostavan način provjere je li vaš poslužitelj osjetljiv na napad:

```
curl -v [IP-adresa-
poslužitelja]/ -H "Host: irrelevant" -H "Range: bytes=0-18446744073709551615"
```

Ako odgovor sa druge strane nije HTTP Error 400, sustav je potencijalno ranjiv. Na sličan način moguće je ispitati i druge aplikacije koje koriste HTTP.sys, no one ne moraju nužno vratiti 400, pa u tom slučaju valja znati interpretirati rezultat.

Najbrži ali ne i najbolji način rješavanja ovog problema je isključiti kernel caching u IIS-u, čime se zaobilazi upravljački program (čija je svrha upravo ubrzavanje obrade HTTP zahtjeva) i otklanja sigurnosni problem, ali se pritom značajno smanjuju performanse samog poslužitelja.

Valja imati na umu da druge aplikacije vjerojatno nemaju opciju isključivanja kernel cachinga, pa je svakako preporučljivo čim, čim prije instalirati zakrpu za ovaj sigurnosni propust.

pon, 2015-04-27 12:08 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Kuharice: Windows [3]
Kategorije: Servisi [4]
Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1544

Links
[1] https://ma.ttias.be/remote-code-execution-via-http-request-in-iis-on-windows/
[2] https://sysportal.carnet.hr/taxonomy/term/13
[3] https://sysportal.carnet.hr/taxonomy/term/18
[4] https://sysportal.carnet.hr/taxonomy/term/28