PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **25** (1997/1998)
Številka 3
Strani 141–143

Martin Juvan in Jože Marinček:

F0 0F C7 C8 IN PROCESOR PENTIUM

Ključne besede: računalništvo, mikroprocesorji, Pentium, napake.

Elektronska verzija:
http://www.presek.si/25/1335-Juvan-Marincek.pdf

F0 0F C7 C8 IN PROCESOR PENTIUM

Proizvajalec mikroprocesorjev in drugih elektronskih komponent družba Intel iz Santa Clare, Kalifornija, ZDA, s svojimi izdelki iz družine Pentium res nima sreče. Pred tremi leti je njegov ugled močno načelo odkritje, da mikroprocesor Pentium količnikov nekaterih parov realnih števil ne izračuna tako natančno, kot bi jih moral. (Članek o matematičnem ozadju odkritja te napake si lahko preberete v tej številki Preseka.) Napaka in predvsem ravnanje Intela ob njenem razkritju sta kupce procesorjev Pentium tako razburila, da je morala družba brezplačno zamenjati vse procesorje z napako. Zaradi zamenjave je nastalo več kot 450 milijonov dolarjev stroškov, taki stroški pa so velik zalogaj tudi za tako veliko podjetje, kot je Intel.

Precej bolj neopazno je maja lani minilo razkritje še ene napake, povezane s predstavitvijo realnih števil v premični piki. Nasledniki procesorjev Pentium, procesorji Pentium Pro in Pentium II, namreč včasih pri pretvarjanju realnih števil v cela "pozabijo" postaviti zastavico za prekoračitev obsega.

V začetku novembra so se novice o procesorjih Pentium spet pojavile tudi v medijih, ki običajno ne poročajo o računalniških dogajanjih. In to za Intel niso bile dobre novice. Kaže, da se je prvo sporočilo o novi napaki v delovanju procesorja Pentium pojavilo 6. novembra. Pošiljatelj je želel ostati anonimen, zato je kot svoj elektronski naslov navedel `noname@noname.com`, sporočilo pa je bilo poslano prek omrežja University of Texas. Dan kasneje je bila na internetu že kopica dodatnih sporočil o napaki, možnih razlogih zanjo, ugibanj o tem, kako bo ravnal Intel itn. Pri Intelu so reagirali umirjeno, njegovi strokovnjaki pa so si vzeli nekaj dni za premislek, predno so uradno "potrdili" (beri: priznali krivdo za) obstoj napake. Vesti o novih težavah s procesorjem Pentium so se hitro pojavile tudi v vseh pomembnejših sredstvih javnega obveščanja. Tako je na primer časnik Delo 13. novembra na prvi strani objavil krajši prispevek o dogodkih, povezanih z odkritjem napake.

In za kakšno napako sploh gre? Poenostavljeno jo lahko razložimo takole. Procesorji iz družine Pentium poznajo ukaz CMPXCHG8B, ki primerja vsebino para registrov s 64-bitno vrednostjo v pomnilniku in glede na izid primerjave opravi ustrezno zamenjavo vsebin (CMP $\equiv$ compare, XCHG $\equiv$ exchange, 8B $\equiv$ 8 zlogov $=$ 64 bitov). Ker je ukaz "zapleten", pri uporabi pa večkrat želimo, da se celotni ukaz izvede brez prekinitev, ki jih povzročajo zunanji signali, mu lahko dodamo še posebno predpono (*lock*), ki zagotovi, da njegovo izvajanje ne bo prekinjeno. Do težav pride, ko zgoraj omenjeni ukaz izvedemo v "zaklenjenem" načinu, kot operand

pa uporabimo enega od registrov. Ker imajo Pentiumovi registri le 32 in ne 64 bitov, med izvajanjem ukaza pride do napake. To ni še nič hudega, saj procesor med izvajanjem ukazov večkrat ugotovi, da ti niso pravilno sestavljeni. Procesor tako opozori na napako in poskuša izvesti poseben podprogram (*error handler*), ki naj bi poskrbel za "odpravo" napake. Ker pa je ukaz izveden v "zaklenjenem" načinu, procesor po prekinitvi izvajanja ukaza omenjenega podprograma ne more izvesti, zato se "obesi". V življenje ga obudi le ponoven zagon računalnika (zadošča pritisk na gumb Reset).

Uradno Intelovo poimenovanje napake je "Invalid Operand with Locked Compare Exchange 8Byte (CMPXCHG8B) Instruction Erratum". Napaka je značilna le za procesorje Pentium, medtem ko starejši (npr. 486) in novejši procesorji (Pentium Pro, Pentium II), zaradi drugačne arhitekture, na kodo, ki povzroči napako, reagirajo pravilno (pokličejo podprogram za "odpravo" napake, nadaljnje ukrepanje pa je odvisno od operacijskega sistema). Napaka za običajnega uporabnika ne predstavlja večje nevarnosti, saj uporabniški programi resnih programerskih hiš ne vsebujejo zlobne oblike ukaza CMPXCHG8B. Pa tudi če do napake pride (recimo, da nam nekdo uspe "podtakniti" pokvarjeno kodo), izgubimo le podatke, ki so se ob nastopu napake nahajali v pomnilniku (niso pa še bili shranjeni na disk). Ker pa vsi vemo, da je redno shranjevanje opravljenega dela ena od osnov varnega dela z osebnim računalnikom, nas taka napaka ne more presenetiti. Napaka je bolj nevarna za večuporabniške računalnike (in za strežnike), saj jo lahko povzroči prav vsak "zloben" uporabnik z možnostjo izvedbe lastne kode, pri čemer ni treba, da ima tak uporabnik tudi kakšne dodatne privilegije.

Približno teden dni po odkritju napake so pri Intelu predstavili svoje predloge za njeno odpravo. Njihovi inženirji so se potrudili in izdelali načrt za programsko odpravo napake. Zavedali so se namreč, da bi pri popravku na nivoju strojne opreme razočarani kupci v velikem številu zahtevali zamenjavo procesorjev, stroški tako številnih zamenjav pa bi lahko resno ogrozili uspešno poslovanje družbe. Pri Intelu so tako pripravili splošna navodila za izdelovalce operacijskih sistemov, vsak izdelovalec pa je zadolžen za izdelavo popravka za svoj operacijski sistem. Intelova rešitev je precej zvita in temelji na nekaterih posebnostih procesorja Pentium. Nekoliko presenetljivo je tudi, da je tako resno napako v strojni opremi mogoče odpraviti kar s spremembo programske opreme, še bolj nenavadno pa je, da programska rešitev praktično ne upočasni delovanja računalnika.

In kako lahko sami preverite, ali imate "pristni" Pentium? Če uporabljate Microsoftov operacijski sistem (MS DOS ali katero od različic Oken),

si lahko pomagate z vgrajenim ukazom debug. Ukaz poženete iz ukazne vrstice in vtipkate podčrtano besedilo, vsako vrstico pa zaključite s pritiskom na tipko Enter (namesto vprašajev bo operacijski sistem izpisal šestnajstiške naslove, ki za nas niso pomembni):

```
C:\> debug
-a100                          Vpisovanje ukazov v zbirniku.
????:0100 db f0 0f c7 c8       Usodni ukaz.
????:0104 ret
????:0105
-g                             Poženemo vpisani program.
```

Pri kodi ukaza lahko namesto c8 vpišete tudi eno od vrednosti c9, ca, ..., cf (gre za šestnajstiške vrednosti, ki določajo različne registre kot operande ukaza). Če imate običajni Pentium, bo računalnik "zamrznil". Če pa delate z drugačnim procesorjem, bo odziv odvisen od operacijskega sistema. V Oknih 95/NT boste dobili obvestilo o napačnem ukazu, okno z ukazno vrstico pa se bo zaprlo. V MS DOS-u pa bo računalnik najverjetneje "obvisel", tipkovnica pa se bo še vedno odzivala. Običajno boste ponovni zagon lahko dosegli že s kombinacijo tipk Control+Alt+Delete. Drugi način, s katerim boste verjetno tudi izzvali napako, je, da prevedete in poženete spodnji enovrstični program v C-ju:

```
unsigned char main[] = { 0xf0, 0x0f, 0xc7, 0xc8 };
```

Tudi proizvajalci strojne opreme počasi postajajo podobni izdelovalcem programske opreme. Slednji so nas že pred časom "navadili" na izdelke z napakami in kopico pomanjkljivosti ter na njihovo nikoli dokončano "razhroščevanje". Zdi se, da se nam sčasoma nekaj podobnega obeta tudi pri strojni opremi za osebne računalnike.

Če radi križarite po internetu, potem si lahko uradne Intelove razlage križev in težav s procesorjem Pentium preberete na naslovu

http://support.intel.com,

zamolčana dejstva pa boste našli na naslovu

http://www.x86.org.

Da ne bo pomote, ločil na koncu obeh naslovov vam ni treba odtipkati.

Martin Juvan, Jože Marinček