Blue Screen Of Death

by m4rk0

1. Uvod

Ukoliko ste ikada koristili Windows OS onda ste verovatno već imali priliku da vidite "Blue Screen Of Death", odnosno BSOD. U ovom tutorijalu ću vam objasniti neke detalje o tome šta zapravo predstavlja BSOD i ponuditi određene opcije koje bi vam mogle pomoći prilikom rešavanja problema. Bitno je znati da, ukoliko je win sistem tako podešen da se usled sistemske greške automatski restartuje, nećete biti u mogućnosti da vidite BSOD, a više informacija ćete naći u event viewer-u. Znači, neophodno je da diseblujete automatski restart nakon greške. Diseblovanje ove opcije pronaćićete u System Properties-u.

1.1 Šta je BSOD

Kada se windows susretne sa situacijom koja onemogućava sistemsku operaciju (na pr: "bug"), dolazi do specifičnog pada sistema. To se još naziva i system crash, kernel error, system fault, ili Stop error.. Tom prilikom se ekran prebacuje u VGA tekst mod, iza je plava pozadina i zatim dolazi do prikazivanja error poruke. Upravo zbog te plave boje u pozadini i naravno njene osobine dobjen je i naziv Blue Screen of Death (BSOD).

1.2 Forma BSOD-a

Izgled tj. forma poruke BSOD-a zavisi od uzroka greske. BSOD može imati sledeću formu:

```
STOP: 0x00000079 (0x00000002,0x00000001,0x00000002,0x00000000)
```

U ovom slučaju prva vrednost (0x00000079 – sve vrednosti u ovom zapisu su hexadecimalne) je poznata kao bugcode ili Stop code. Ostale četiri cifre (bez zagrada) čine BSOD listu parametara i imaju vrednosti koje su zavisne od bugcod-a..

Druga forma BSOD –a je:

```
STOP: c000021a (Fatal System Error).
```

Pored navedenih, i druge hexadecimalne informacije mogu biti prikazane u BSOD-u.

One mogu sadržati:

- Naziv drajvera ili servisa koji je izazvao BSOD
- Tekstualno objašnjenje razloga nastanka BSOD-a
- Moguće načine popravke
- Kernel deo memorije sa adresama

Postoji preko 250 dokumentovanih BSOD kodova i mnogi od njih su dokumentovani samo kao "This bug check appears very infrequently." (ovo je celokupan tekst citiran direktno iz Microsoft dokumentacije). I nažalost, većina BSOD kodova sadrže nelogi;ne adrese tako da je slaba vajda od njih.. Iz ovoga zaključujemo da u okviru BSOD-a možemo pronaći samo deo uzroka pada sistema, i neophodno je znatno dublje istraživanje.

The Microsoft Device Driver Kit (poznatiji kao DDK) navodno sadrži listing svih dokumentovanih BSOD bugkodova. Ipak, činjenica je da postoji više bugkodova od onih koji su dokumentovani u DDK.

1.3 Lista najčešćih uzročnika BSOD-a

Postoji opšteprihvaćena lista uzročnika koji najčešće izazivaju BSOD. S tim u vezi, bitno je da korisnici budu obazrivi sa 3rd party hardverom i drajverima koji nisu WHQL sertifikovani.

U ovu listu spadaju:

- CDROM/CD-RW/DVD-RW
- Eksterni hard diskovi
- Antivirusni programi
- Eksterni uređaji za bekap
- Programi za "održavanje" grafike.

2. Pojava BSOD-a, načini popravke i Kernel terminologija

2.1 Pojava

Kada se BSOD pojavi, započeta operacija na sistemu se ne može nastaviti. Većina BSOD-a ne izaziva oštećenje podataka, pogotovo ako je u pitanju NTFS file sistem. Ukoliko se javi bugcheck, korisnik bi na osnovu njega trebao da otkrije način da reši problem i takođe da otkrije koji softver ili drajver može biti uzročnik greške. Ukoliko na BSOD ekranu primetite neke podatke i u njima naziv nekog drajvera, upravo taj drajver je potencijalni izazivač problema.

2.2 Načini popravke

U suštini nema baš mnogo načina otklanjanja greške i uglavnom svako pokuša jednostavan restart što za divno čudo ponekad i reši problem. Ukoliko se i posle toga BSOD pojavi, potrebno je izvesti određene korake. Ukoliko smo skoro instalirali neki softver ili ubacivali nešto od hardvera potrebno je proveriti da nešto od toga nije izvor problema. Svi win useri bi trebali da obrate pažnju na softver koji instaliraju i da budu obazrivi sa driverima koji nisu WHQL sertifikovani.

Treba uraditi sledeće:

- Proveriti u event viwer-u da nema neka prijavljena greska
- Pokrenuti **`Chkdsk/f/r`** i proveriti sve particije..

Btw: ukoliko su vam particije formatirane u FAT, određeni fajlovi koje win koristi mogu biti uništeni ako se scandisk ili drugi MS-DOS bazirani HD toolovi pokrenu iz cmd-a. Uvek koristiti verziju Chkdsk koja odgovara verziji vašeg win-a., a to se obično ovde nalazi: **`C:\winnt\system32 ili %SystemRoot%\system32`**.

2.2.1 Novi hardver dodat ili je postojeći modifikovan

Prvo ćemo početi od slučaja kada je novi hardver dodat ili je postojeći modifikovan.

U ovom slučaju treba uraditi sledeće:

- Pokrenuti soft koji dobijate uz hardver od strane proizvođaca
- Proverite sve konatkte, kablove ulaze/izlaze itd.
- Proveriti da li su instalirani latest driveri i da li je instaliran poslednji sp za win.
- Proveriti System Log u Event Viewer-u da li je "pribeležen" neki error.
- Ukloniti sumnjiv drajver ili uređaj, restartovati komp i proveriti da li je problem rešen.

2.2.2 Popravka putem safe mode-a

Pri podizanju win-a pritiskajte f8 i pojaviće vam se safe mod screen sa nekoliko ponuđenih opcija Ako se BSOD javio nakon instalacije novih ili apdejtovanih drajvera, ti drajveri bi trebali da se uklone ili zamene odgovarajućima. Ukoliko se BSOD javio za vreme startup procesa, bićete u mogućnosti da upotrebite Safe Mode booting da biste preimenovali i/ili izbrisali drajver koji je uzročnik problema..U safe mod screenu se može izabrati i Last Known Good Configuration, čijim će se odabirom učitati system sa poslednjom konfiguracijom koja je radila ok.

2.2.3 Identifikacija drajvera

Pri BSOD-u će se u error-u identifikovati uređaj koji je izazvao problem. U tom slučaju treba ukloniti taj uređaj i izbrisati njegove drivere. Da biste saznali da li je driver iz m$ paketa, obratite pažnju na donju tabelu.

Lista NT drajvera koji se mogu javiti u BSOD-u:

Naziv drivera	Funkcija
NtosKrnl.exe	NT kernel
NTdll.dll	NT support library
Win32k.sys	Graphics Display Interface (GDI) Driver
Hal.dll	Hardware Abstraction Library

2.3 Kernel terminologija

- **Bugcode** - Heksadecimalna vrednost koja identifikuje BSOD. Primer je 0xA, koji identifikuje ovaj BSOD kao IRQL_NOT_LESS_OR_EQUAL BSOD
- **Driver** - Ovo je kernel mode program koji je deo Windows OS-a i koji upravlja svim zahtevima kod određenih uređaja. Na pr display driver koji "sakuplja" komande sa win aplikacija i prosledjuje hardveru sta da "iscrta" na ekranu.

- **Exception** - Error uslovljen drajverom koji izaziva gresku ili pad sistema

- **HCT** - Hardware Compatibility Test. Ovo je veoma važan Microsoft validation test za drajvere koji, ukoliko su ga prošli, omogućava istima da budu smešteni u Microsoft's Hardware Compatibility Listu. Ukoliko je drajver uspešno prošao HCT, veoma je mala verovatnoća da je upravo on uzročnik BSOD-a.

- **HCL** - Hardware Compatibility List. Ovo je m$ lista sertifikovanih drajvera koji su prošli Hardware Compatibility Test (HCT).

- **IRQL** - Interrupt ReQuest Level. U toku procesa, NT kernel će proći kroz različite oblike. Ovi oblici su poznati kao IRQL i identifikovani su kompletom celih brojeva i to od 0 do 31. Kod svakog IRQL postoje specifična pravila kojih se moramo pridržavati.. Na pr određene memorijske reference mogu jedino biti izvršene kod odredjenog IRQL-a, a kod ostalih to neće biti slučaj.

- **IRP** - I/O Request Packet. Standardni paket I/O zahteva koji se šalju drajverima. Tipični I/O zahtevi trebali bi predstavljati aktivnosti kao što su: čitati, pisati, otvarati, zatvarati..

- **onPaged Pool** - Ovo je područje kernel memorije koje ne može da bude “adresirano” izvan memorije (na pr:, Paged Pool). Obično će drajver odvojiti takvu memoriju tako da će moći da pristupi bilo kom IRQL.

- **NT kernel** - Generično ime za Windows operativne sisteme posle Win3x/Win9x. On uključuje Windows NT 4, Windows 2000, Windows XP i Windows .NET

- **Paged Pool** - Ovo je područje kernel memorije koje može biti “adresirano” van diska ukoliko ono nije trenutno upotrebljeno, tj. zauzeto.

- **Service ili System Service** - Ovo je program koji nije deo kernela i koji izvršava zadatke u korist drugih procesa. Korisnik ne može direktno pristupiti ovom servisu, ali zato programi/aplikacije mogu da zadaju zahtev servisima za njihovo izvršavanje.

- **WinDBG** - Ovo je Windows Kernel Mod debugger koji je ekvivalentan naprednim verzijama sledećih debuggera UNIX sistema: dbx, gdb, kdb, kgdb.

- **Wintel -** Stenografija za Windows/Intel**.**

3 BSOD - Objašnjenja

U nastavku ću vam izneti BSOD poruke koje se uglavnom javljaju. Sami vidite da se pri erroru javlja određen pojam koji opisuje i sam problem. Na pr “file system error” znači da nešto nije uredu sa sistemskim fajlovima itd.

3.1 Bugcode 0xA - IRQL_NOT_LESS_OR_EQUAL

Ovaj BSOD se javlja pri pokušaju pristupa netačnoj adresi memorije.

Parametri:
1 * adresa na koju je neispravno upućeno.
2 * IRQL koji se zahteva za pristup memoriji
3 * tip pristupa, pri čemu 0 označava operaciju čitanja, a 1 operaciju pisanja.
4 * adresa uputstva koja upućuje na memoriju u parametru 1

Popravka:
- Last Known Good Configuration
- Repair sistema
- Roll Back Driver
- Recovery konzola
- Ispitati nedavno instalirani hardver

3.2 Bugcode 0x1E - KERNEL_MODE_EXCEPTION_NOT_HANDLED

Javlja se kada program za obradu grešaka ne prihvati grešku napravljenu od strane drajvera. Znači, nastaje kada se opozove loša memorijska adresa.

Parametri:
1 * exception code
0x80000002 = unaligned data reference encountered
0x80000003 - a kernel breakpoint/ASSERT encountered
0xC0000005 - dogodio se zabranjen pristup memoriji
2 * adresa greške
3 * parametar 0 greške
4 * parametar 1 greške

Popravka:
- Proveriti da li su instalirani latest drajveri za ploču
- Ukoliko su u skorije vreme instalirani sumnjivi drajveri ili softver, treba se obratiti posebna pažnja.
- Erorr se javlja posle prvog restarta i to za vreme učitavanja Windowsa ili nakon završetka učitavanja. Takođe se može javiti ukoliko nema dovoljno mesta na disku za instalaciju. U tom slučaju izbrišite sve nepotrebne stvari koje vam nisu potrebne, tipa temp fajlovi i ostali trash.

3.3 Bugcode 0x2E - DATA_BUS_ERROR

Javlja se kada je error detektovan u sistemskoj memoriji a problem je hardverske prirode, tj. kad je ubačeni hardware oštećen ili nije dobro podesena konfiguracija za njegov rad. Najčešće su u pitanju: oštećena radna memorija, Level 2 RAM cache greške, ili video RAM greške. Takođe i HD može biti krivac ovog BSOD-a.

Parametri:
1 * Virtualna adresa koja je izazvala kvar
2 * Fizička adresa koja je izazvala kvar
3 * Processor status register (PSR)
4 * Faulting instruction register (FIR)

Popravka:
- Postoji mogućnost da novi hardver nije dobro podešen, stoga rešenje potražite u odeljku „Novi hardver dodat ili je postojeći modifikovan“
- Proveriti system dal nema virusa i ostale gamadi
- Odraditi `Chkdsk/f/r` (kucati u command promptu) na sistemskoj particiji.

3.4 Bugcode 0x3F - NO_MORE_SYSTEM_PTES

Javlja se kada system izvrši previše I/O akcija i tada dolazi do fragmentovanja "system page tabele" - (PTE). To se dešava ukoliko odgovarajući drajver ili aplikacija nije uklonjens kako treba.

Parametri:
1 * tip PTE-a , gde 0 predstavlja ekspanziju sistema , a 1 predstavlja ekspanziju nonpaged pool-a.
2 * veličina memorijskog zahteva
3 * ukupno slobodnih PTE-sa
4 * ukupno PTE-sa

Popravka:
- Ukloniti sav softver koji ste instalirali u skorije vreme, a posebno backup aplikacije.

3.5 Bugcode 0x22 - FILE_SYSTEM

Javlja se usled greške kod sistemskih fajlova. Javlja se u slučajevima kada se set sistemskih fajlova razlikuje od onog kada system normalno funkcioniše i razlog ove greške su oštećeni dll fajlovi kao i softver kupljen na buvljaku :>.

Parametri:
1 * broj linije/oznake ugrađenog modula
2 * nije upotrebljen
3 * nije upotrebljen
4 * nije upotrebljen

Popravka:

- Repair/clean install.

3.6 Bugcode 0x44 - MULTIPLE_IRP_COMPLETE_REQUESTS

Višestruki zahtev za završetkom slanja IRP-a (I/O Request Packet). Što se tiče popravke, korisnik treba da obrati pažnju na sve aplikacije koje su pokrenute u trenutku pada sistema.

Parametri:
1 * IRP adresa
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:
- Nema popravke.

3.7 Bugcode 0x4E - PFN_LIST_CORRUPT

Dolazi do oštećenja Page Frame Number (PFN) liste. Što se tiče popravke, korisnik treba da obrati pažnju na sve aplikacije koje su pokrenute u trenutku pada sistema.

Parametri:
1 * tip oštećenja
2 * PFN u trenutku greške.
3 * informacije o strani
4 * Rezervisan

Popravka:
- Nema popravke.

3.8 Bugcode 0x5 - INVALID_PROCESS_ATTACH_ATTEMPT

Ovo ukazuje da kernel proces pokušava da se poveže sa drugim procesom. Ova greška posebno utiče na win server. Što se tiče popravke, korisnik treba da obrati pažnju na sve aplikacije koje su pokrenute u trenutku pada sistema.

Parametri:
1 * Rezervisan
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:
- Nema popravke.

3.9 Bugcode 0x50 - PAGE_FAULT_IN_NONPAGED_AREA

Javlja se kada drajver pokuša da pristupi memoriji kojoj se ne može pristupiti u trenutnom IRQL-u. Sistem će pružiti informacije isticanjem naziva drajvera koji je uzrok BSOD-a.

Parametri:
1 - adresa na koju je upućeno
2 - tip pristupa, pri čemu 0 označava operaciju čitanja, a 1 operaciju pisanja.
3 - adresa uputstva koja upućuje na memoriju u parametru 1
4 - rezervisan

Popravka:

- Postoji mogućnost da novi hardver nije dobro podešen, stoga rešenje potražite u odeljku Novi hardver dodat ili je postojeći modifikovan
- Ako imate instaliran antivirus, sprečite da vrši skeniranje, a ako se i posle toga problemi nastave, potpuno uklonite antivirus.

3.10 Bugcode 0x7B - INACCESSIBLE_BOOT_DEVICE

Ovaj error znači da windows ne može da pristupi sistemskoj particiji za vreme setup/boot-a.

Parametri:
1 * rezervisan
2 * 0
3 * 0
4 * 0

Popravka:

- Ovaj error nastaje kada se user ne pridržava instrukcija u toku instalacije. Umesto toga korisnik pokušava da instalira Windows koristeći Microsoft supplied installer (na pr: setup.exe or winnt.exe u I386 direktorijumu instalacionog medija). Razlog nastanaka ovog BSOD-a je taj što PC proizvodi upotrebljavaju “emulated” disk gde postoje posebni drajveri koji se moraju naći u Windows boot-u da bi iščitali informacije na tom disku. Oni nisu prihvaćeni ni na jednoj m$ distribuciji. Popravka se u ovom slučaju vrši restartom u toku instalacije upotrebom "the outlined# metode. Ovaj BSOD se može javiti i nakon uspešne instalacije, znači ne mora biti slučaj kao što sam gore pomenuo. U tom slučaju butujte system sa win diska i u recovery konzolu kucajte Chkdsk

3.11 Bugcode 0x7F - UNEXPECTED_KERNEL_MODE_TRAP

Greška se javila od strane CPU-a i krenel ne uspeva da izbegne taj neočekivan prekid. Postoje prvi i drugi nivo prekida koji kasnije izazivaju errore koji se nadovezuje na ranije errore što se najčešće završava krashom sistema..

Parametri:

1 * broj prekida
0x000000000 - "deljenje nulom" greska
0x000000004 - prekoračenje (owerflow)
0x000000005 - "Bounds check" greška
0x000000006 - neispravan Opcode
0x000000008 - Dvostruke/višestruke greške
2 * rezervisan
3 * rezervisan
4 * rezervisan

Popravka:

- Postoji mogućnost da novi hardver nije dobro podešen, stoga rešenje potražite u odeljku Novi hardver dodat ili je postojeći modifikovan.

3.12 Bugcode 0x8E - KERNEL_MODE_EXCEPTION_NOT_HANDLED

Javlja se kada program za obradu grešaka ne prihvati grešku napravljenu od strane drajvera. Znači, nastaje kada se opozove loša memorijska adresa.

Parametri:

1 * exception code
0x80000002 - unaligned data reference encountered
0x80000003 - a kernel breakpoint/ASSERT encountered
0xC0000005 - memory access violation occurred
2 * adresa na koju je upućen zahtev
3 * moment prekida
4 * Rezervisan

Popravka:

- Proveriti da li su instalirani latest drajveri za ploču
- Ukoliko su u skorije vreme instalirani sumnjivi drajveri ili softver, treba se obratiti posebna pažnja.
- Erorr se javlja posle prvog restarta i to za vreme učitavanja Windowsa ili nakon završetka učitavanja. Takođe se može javiti ukoliko nema dovoljno mesta na disku za instalaciju. U tom slučaju izbrišite sve nepotrebne stvari koje vam nisu potrebne, tipa temp fajlovi i ostali trash.

3.13 Bugcode 0xC000021A - STATUS_SYSTEM_PROCESS_TERMINATED

Ističe da se greška javila u grafičkom podsistemu. Win zahteva da grafički podsistem normalno radi da bi win nastavio operaciju. Najčešće će drajver koji je krivac za nastanak problema biti identifikovan kao winlogon.exe sto u prevodu znaci da je doslo do oštećenja win32k.sys fajla..

Parametri:
1 * Rezervisan
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:

- Ova greška se popravlja jednostavnim restartom, a ako se tim putem ne dodje do rešenja neophodno je pokrenuti `Chkdsk/f/r` radi detektovanja i ispravljanja bilo kog fajla koji je oštećen.

3.14 Bugcode 0xC0000221 - STATUS_IMAGE_CHECKSUM_MISMATCH

Drajver ili sistemska biblioteka je oštećena na disku. Ovo se retko javlja i samo nekoliko puta je primećeno. Javlja se pri grešci u toku prenošenja image podataka sa emulated diska na win os.

Parametri:
1 * Rezervisan
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:

- Ova greska se popravlja jednostavnim restartom, a ako se tim putem ne dođe do resenja neophodno je pokrenuti `Chkdsk/f/r` radi detektovanja i ispravljanja bilo kog fajla koji je oštećen.

3.15 Bugcode 0xD1 - DRIVER_IRQL_NOT_LESS_OR_EQUAL

Drajver pokušava da pristupi memoriji dok je CPU u neodgovarajućem IRQL adresi, tj. do[lo je do poreme'aja mapiranja IRQL adresa u operativnom sistemu.

Parametri:
1 * adresa na koju je neispravno upućeno.
2 * IRQL koji se zahteva za pristup memoriji
3 * tip pristupa, pri čemu 0 označava operaciju čitanja, a 1 operaciju pisanja.
4 * adresa uputstva koja upućuje na memoriju u parametru 1

Popravka:

- Nema popravke.

3.16 Bugcheck 0xC2 - BAD_POOL_CALLER

Kernel tred/proces pruža pogrešno memorijsko odobrenje zahteva.

Parametri:
1 * Rezervisan
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:
- Nema popravke.

3.17 Bugcheck 0xC4 - DRIVER_VERIFIER_DETECTED_VIOLATION

Driver Verifier facility (DVF) je detektovala da uređaj nije prošao verifikaciju od strane driver verifier-a.

Parametri:
1 * Error code
2 * Rezervisan
3 * Rezervisan
4 * Rezervisan

Popravka:
- Javlja se samo u slučaju da je DVF enablovan. Driver Verifier je takođe i automatski enablovan u toku rada Microsoft Hardware Compatibility Test-a (HCTs). Rešenje je jednostavno udariti disable i to je to.