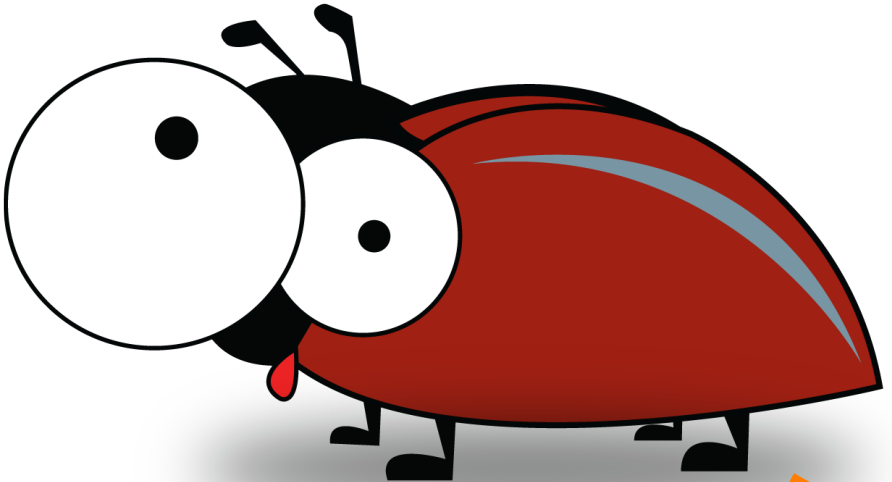
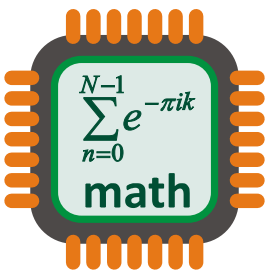
Microcode updates as protection against Spectre & Co.

@wefinet
Werner Fischer

DENOG 11
GERMAN NETWORK OPERATORS GROUP

THOMAS KRENN®

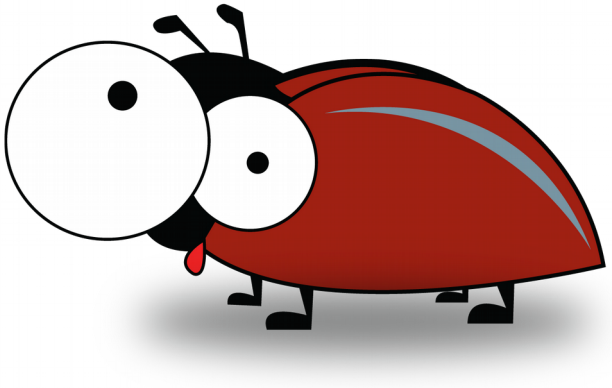




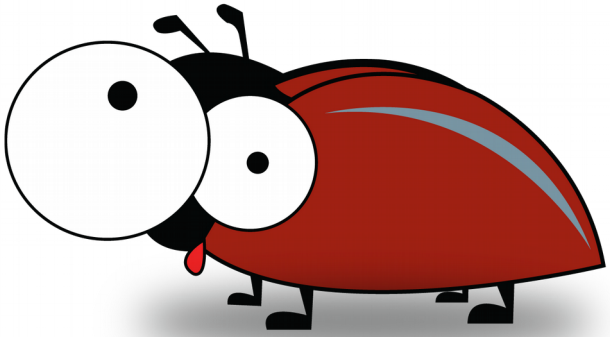
Houses

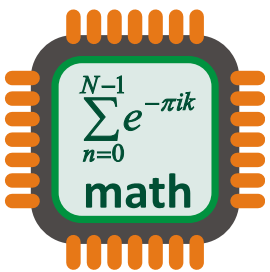
Software

Hardware



Software





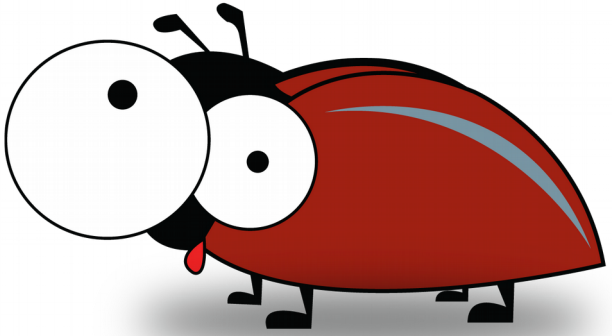
Hardware

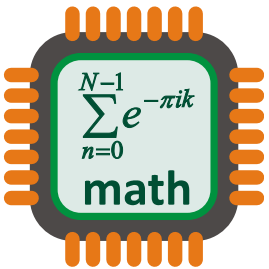
FDIV Replacement Program

In December of 1994, Intel announced a lifetime replacement policy on the well publicized floating point unit flaw, contained in the then current version (60-100MHz) of the Pentium® processor. Non-FPU flawed versions of the Pentium processor began shipping in late 1994. If you took delivery of your system on Jan 1, 1995 or later, it is increasingly probable that you have a processor without the flaw. Therefore, it is important that you check your system to determine if a replacement is needed. See question 2 in the FAQs to find out how you can easily check your system for the flaw.

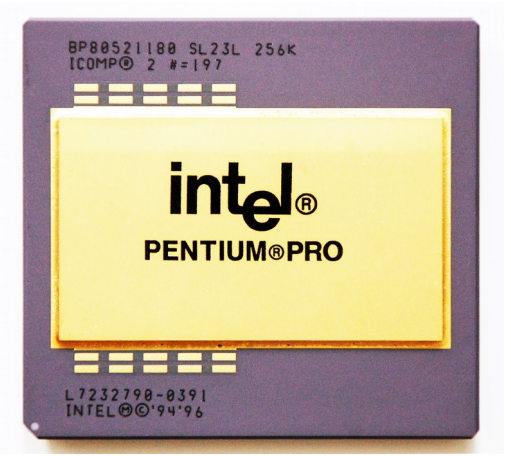
The replacement program is directed at End Users of working systems who are concerned about the impact of this flaw on their applications (see White Paper for more information). The FAQ describes the replacement process as well as answers commonly asked questions. In addition to this guide, you can call the customer service numbers for information regarding the replacement program.

- Frequently Asked Questions (updated - 14 May 98) about the Pentium® processor replacement program
- Intel® Processor Frequency ID Utility: a utility that will identify the Intel processor contained in your PC
- Customer Service Telephone Numbers for replacement
- Intel White Paper: Detailed Statistical Analysis of Floating Point Flaw in Pentium Processors

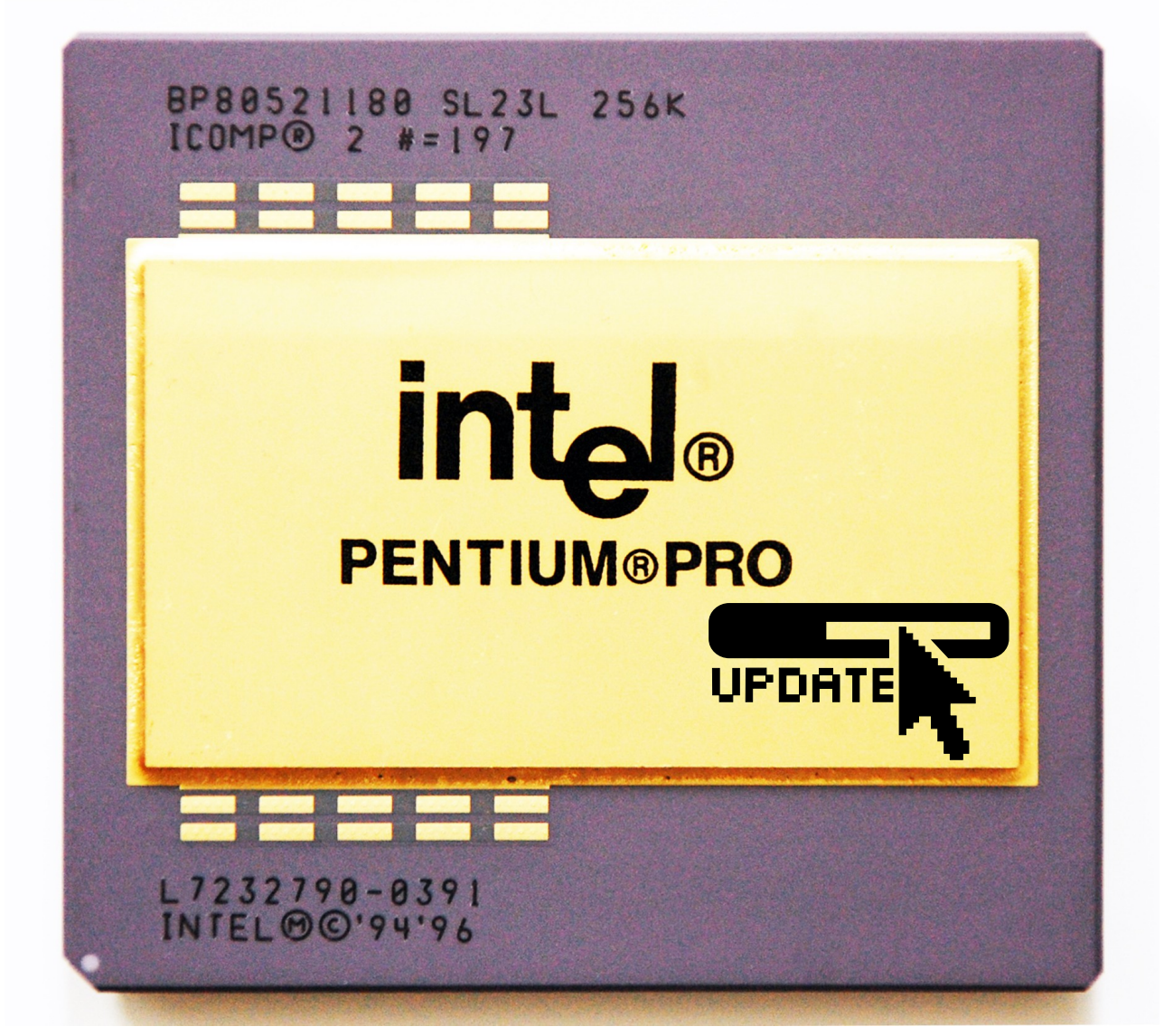




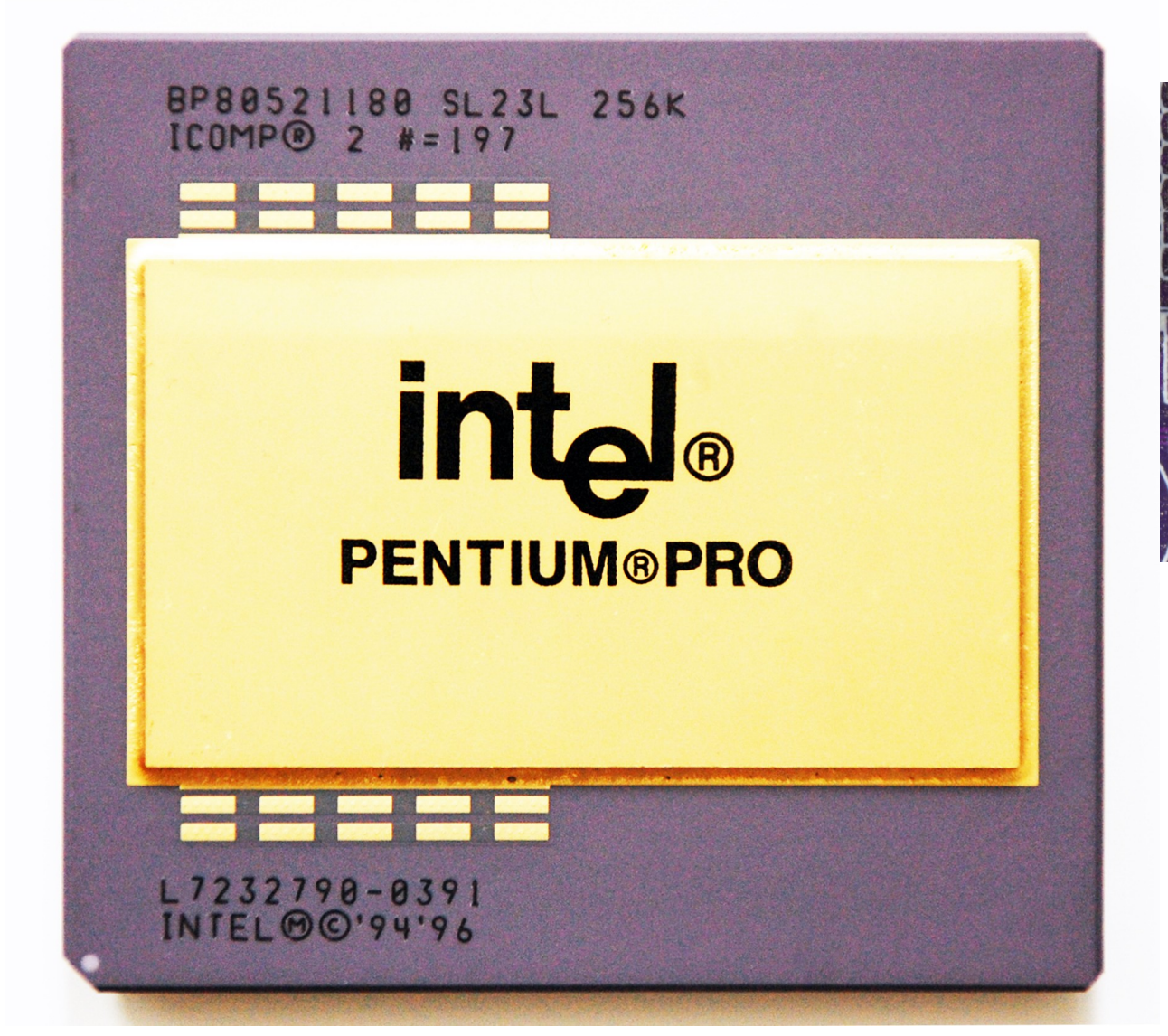
Hardware



Microcode
:-)

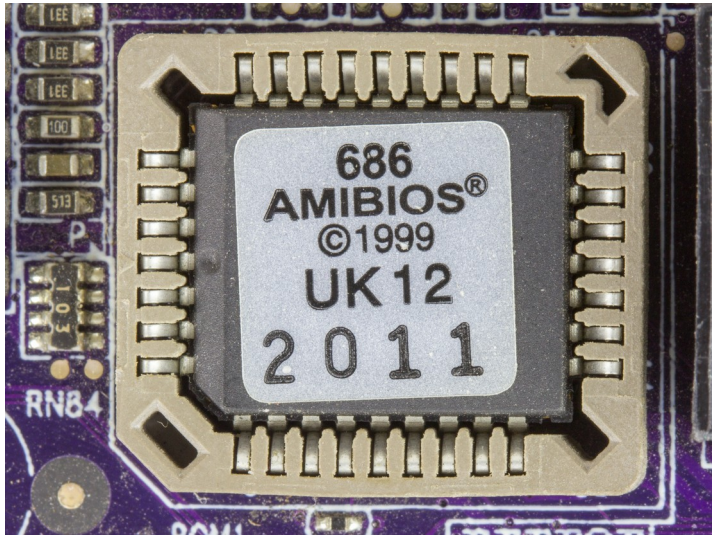

BP80521180 SL23L 256K
ICOMP® 2 #=197
intel®
PENTIUM®PRO
UPDATE
L7232790-0391
INTEL©'94'96

?


BP80521180 SL23L 256K
ICOMP® 2 #=197
intel®
PENTIUM®PRO
L7232790-0391
INTEL©'94'96


686
AMIBIOS®
©1999
UK12
2011
RN84


UPDATE




```
MC Extractor v1.32.0 r107

X11DPi-N9.401 (1/1)
```

Intel								
#	CPUID	Platform ID	Revision	Date	Type	Size	Offset	Last
1	50654	B7 (0,1,2,4,5,7)	200005A	2019-01-28	PRD	0x8400	0x1D96700	No
2	50655	B7 (0,1,2,4,5,7)	3000010	2018-11-16	PRD	0xB800	0x1D9EB00	Yes
3	50656	BF (0,1,2,3,4,5,7)	4000021	2019-02-27	PRD	0xB800	0x1DAA300	Yes
4	50657	BF (0,1,2,3,4,5,7)	5000021	2019-02-27	PRD	0xB800	0x1DB5B00	Yes

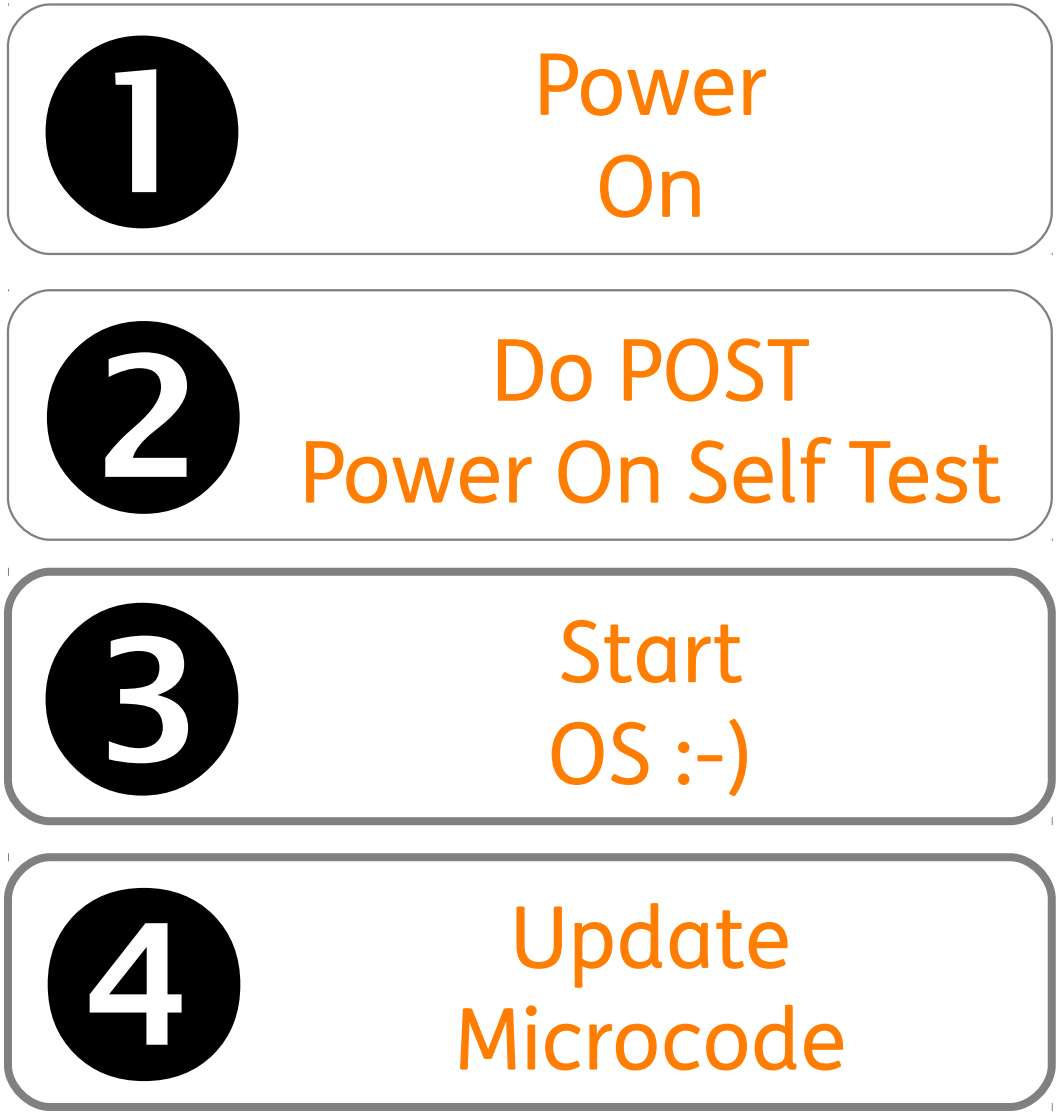
```
Press enter to exit
```


1
Power
On
2
Do POST
Power On Self Test
3
Update
Microcode
4
Start
OS :-)

BUT: Do you …

… like BIOS Updates?

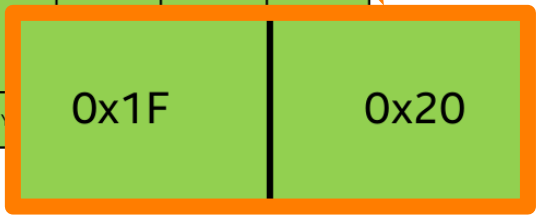
… like SW Updates?


1
Power
On
2
Do POST
Power On Self Test
3
Start
OS :-)
4
Update
Microcode

```
wfischer@tpw: ~
wfischer@tpw:~$ iucode_tool --scan-system
iucode_tool: system has processor(s) with signature 0x000306a9
wfischer@tpw:~$
```

MICROCODE UPDATE GUIDANCE

Code Name	Product Collection	Product Names	Vertical Segment	CPUID	Platform ID	[illegible] date for Q2	Production Status	Pre-Mitigation Production MCU	New Production MCU Rev
Ivy Bridge	3rd Generation Intel® Core™ Processor Family Intel® Pentium® Processor Family Intel® Celeron® Processor Family	Intel® Core™ Processor Extreme Edition i7-3920XM, i7-3940XM Intel® Celeron® Processor 1000M, 1005M, 1007U, 1017U, 1019Y, 1020E, 1020M, 1037U, 1047UE, 927UE, G1610, G1610T, G1620, G1620T, G1630 Intel® Core™ Processor i7-3517U, i7-3517UE, i7-3520M, i7-3537U, i7-3540M, i7-3555LE, i7-3610QE, i7-3610QM, i7-3612QE, i7-3612QM, i7-3612QM, i7-3615QE, i7-3615QM, i7-3630QM, i7-3632QM, i7-3632QM, i7-3635QM, i7-3667U, i7-3687U, i7-3689Y, i7-3720QM, i7-3740QM, i7-3770, i7-3770K, i7-3770S, i7-3770T, i7-3820QM, i7-3840QM Intel® Core™ Processor i5-3210M, i5-3210M, i5-3230M, i5-3230M, i5-3317U, i5-3320M, i5-3330, i5-3330S, i5-3337U, i5-3339Y, i5-3340, i5-3340M, i5-3340S, i5-3350P, i5-3360M, i5-3380M, i5-3427U, i5-3437U, i5-3439Y, i5-3450, i5-3450S, i5-3470, i5-3470S, i5-3470T, i5-3475S, i5-3550, i5-3550S, i5-3570, i5-3570K, i5-3570S, i5-3570T, i5-3610ME Intel® Core™ Processor i3-3110M, i3-3120M, i3-3120ME, i3-3130M, i3-3210, i3-3217U, i3-3217UE, i3-3220, i3-3220T, i3-3225, i3-3227U, i3-3229Y, i3-3240, i3-3240T, i3-3245, i3-3250, i3-3250T Intel® Pentium® Processor 1405 v2, 2020M, 2030M, 2117U, 2127U, 2129Y, A1018, G2010, G2020, G2020T, G2030, G2030T, G2100T, G2120, G2120T, G2130, G2140	Mobile	306A9	12	Yes	Production	0x1F	0x20
Ivy Bridge E	Intel® Core™ X-series Processors	Intel® Core™ Processor Extreme Edition i7-4960X Intel® Core™ Processor i7-4820K, i7-4930K	Desktop	306E4	ED	[illegible]			



Linux* Processor Microcode Data File

Version: Latest (Latest) Date: 8/7/2018

Available Downloads

Linux*

Language: English

Size: 1.55 MB

MD5: b12f8680d87c81a302e8c85712ed1a80

microcode-20180807a.tgz

Other Versions

microcode-20190312

20180703

20180425

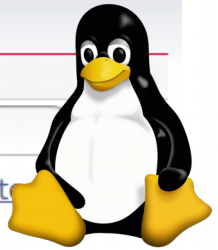
Detailed Description

Intel Processor Microcode Package for Linux*

CPU microcode is a mechanism to correct certain errata in existing systems. The normal preferred method to apply microcode updates is using the system BIOS, but for a subset of Intel's processors this can be done at runtime using the operating system. This package contains those processors that support OS loading of microcode updates.

The target user for this package are OS vendors such as Linux* distributions for inclusion in their OS releases. Intel recommends getting the microcode using the OS vendor update mechanism. Expert users can of course update their microcode directly outside the OS vendor mechanism. This method is complex and thus could be error prone.

Microcode is best loaded from the BIOS. Certain microcode must only be applied from the BIOS. Such processor microcode updates are never packaged in this package since they are not appropriate for OS distribution. An OEM may receive microcode packages that might be a superset of what is contained in this package.



Package: intel-microcode (3.20180807a.2~deb9u1) [non-free]

Processor microcode firmware for Intel CPUs

This package contains updated system processor microcode for Intel i686 and Intel X86-64 processors. Intel releases microcode updates to correct processor behavior as documented in the respective processor specification updates.

For AMD processors, please refer to the amd64-microcode package.

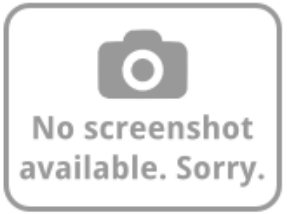
Tags: Hardware Enablement: Need an extra tag, Role: Application Data, Purpose: Hardware Driver

Other Packages Related to intel-microcode

● depends ■ recommends ◆ suggests ▲ enhances

- ● **dep: iucode-tool (>= 1.0)**
  Intel processor microcode tool
- ■ **rec: initramfs-tools (>= 0.113~)**
  generic modular initramfs generator (automation)

Links for intel-microcode



Debian Resources:

- Bug Reports
- Developer Information
- Debian Changelog
- Copyright File

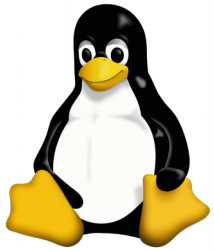
Download Source Package intel-microcode:

- [intel-microcode_3.20180807a.2~deb9u1.c
- [intel-microcode_3.20180807a.2~deb9u1.t

Maintainers:

- Henrique de Moraes Holschuh (QA Page)
- Giacomo Catenazzi (QA Page)

External Resources:



```
wfischer@tpw: ~
wfischer@tpw:~$ dmesg | grep microcode
[    0.000000] microcode: CPU0 microcode updated early to revision 0x20, date = 2018-04-10
[    0.113988] microcode: CPU2 microcode updated early to revision 0x20, date = 2018-04-10
[    0.969048] microcode: CPU0 sig=0x306a9, pf=0x10, revision=0x20
[    0.969057] microcode: CPU1 sig=0x306a9, pf=0x10, revision=0x20
[    0.969061] microcode: CPU2 sig=0x306a9, pf=0x10, revision=0x20
[    0.969070] microcode: CPU3 sig=0x306a9, pf=0x10, revision=0x20
[    0.969105] microcode: Microcode Update Driver: v2.01 <tigran@aivazian.fsnet.co.uk>, Peter Oruba
wfischer@tpw:~$
```

```
root@freebsd12:~ # dmesg
---<<BOOT>>---
Copyright (c) 1992-2018 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
FreeBSD is a registered trademark of The FreeBSD Foundation.
FreeBSD 12.0-RELEASE-p2 GENERIC amd64
FreeBSD clang version 6.0.1 (tags/RELEASE_601/final 335540) (based on LLVM 6.0.1)
VT(efifb): resolution 800x600
CPU: Intel(R) Celeron(R) CPU G1820T @ 2.40GHz (2394.52-MHz K8-class CPU)
  Origin="GenuineIntel"  Id=0x306c3  Family=0x6  Model=0x3c  Stepping=3
  Features=0xbfebfbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,
PAT,PSE36,CLFLUSH,DTS,ACPI,MMX,FXSR,SSE,SSE2,SS,HTT,TM,PBE>
  Features2=0x4ddaebbf<SSE3,PCLMULQDQ,DTES64,MON,DS_CPL,VMX,EST,TM2,SSSE3,SDBG,CX16,
xTPR,PDCM,PCID,SSE4.1,SSE4.2,MOVBE,POPCNT,TSCDLT,XSAVE,OSXSAVE,RDRAND>
  AMD Features=0x2c100800<SYSCALL,NX,Page1GB,RDTSCP,LM>
  AMD Features2=0x21<LAHF,ABM>
  Structured Extended Features=0x2603<FSGSBASE,TSCADJ,ERMS,INVPCID,NFPUSG>
  Structured Extended Features3=0x9c000000<IBPB,STIBP,L1DFL,SSBD>
  XSAVE Features=0x1<XSAVEOPT>
  VT-x: PAT,HLT,MTF,PAUSE,EPT,UG,VPID
  TSC: P-state invariant, performance statistics
real memory  = 2147483648 (2048 MB)
avail memory = 2002997248 (1910 MB)
CPU microcode: updated from 0x24 to 0x25
Event timer "LAPIC" quality 600
```

platomav / **CPUMicrocodes**

Watch 28 | Unstar 163 | Fork 23

Code | Issues 0 | Pull requests 0 | Wiki | Insights

Intel, AMD & VIA CPU Microcode Repositories

57 commits | **1** branch | **0** releases | **1** contributor

Branch: **master** | New pull request | Create new file | Upload files | Find File | Clone or download

platomav Updated to MCE DB r109 — 1 — Latest commit 8b0b9ab 6 days ago

AMD	Updated to MCE DB r101	2 months ago
Intel	Updated to MCE DB r109	6 days ago
VIA	Updated to MCE DB r52	a year ago
README.md	Update README.md	7 months ago

README.md

CPUMicrocodes

Intel, AMD & VIA CPU Microcode Repositories

CPU Microcode Repositories News Feed

CPU Microcode Repositories Discussion Topic

MC Extractor

MC Extractor Discussion Topic

This is a collection of every **Latest Production** Intel, AMD and VIA CPU microcode we have found. You can use MC Extractor to check instantly whether a microcode is already at the repository.

MC Extractor v1.24.5

MC Extractor v1.24.5 r97

Intel

#	CPUID	Platform ID	Revision	Date	Type	Size	Offset	Last
1	50654	B7 (0,1,2,4,[illegible],7)	2000059	2018-12-20	PRD	0x8000	0x1C890B0	Yes
2	50655	B7 (0,1,2,4,5,[illegible])	300000F	2018-10-08	PRD	0xB400	0x1C910B0	No
3	50656	BF (0,1,2,3,4,5,[illegible]	4000010	2018-11-06	PRD	0xC000	0x1C9C4B0	No
4	50657	BF (0,1,2,3,4,5,7)	[illegible]000010	2018-11-06	PRD	0xC000	0x1CA84B0	No

Note: Microcode #1 was not found at the database, please report it!

Note: Microcode #2 was not found at the database, please report it!

Note: Microcode #3 was not found at the database, please report it!

Note: Microcode #4 was not found at the database, please report it!

Am I secure now?

THOMAS KRENN®

Allianz für Cyber-Sicherheit
Partner

THOMAS KRENN®

→ Update Microcode via OS

→ Still check for BIOS updates

THOMAS KRENN®