

# RE: Portcullis Security Advisory 05-011 ACPI 1.6 BIOS

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-03/0516.html>

---

*From:* Paul J Docherty (*PJD\_at\_portcullis-security.com*)

*Date:* 03/30/05

Date: Wed, 30 Mar 2005 08:31:01 +0100

To: "Kurt Seifried" <bt@seifried.org>, "bugs" <bugs@securitytracker.com>, "Bugtraq" <bugtraq@secu

Hi Kurt,

Fdisk /MBR only replaces the boot code within the sector, it does not change in any way the Partition Information Block (PIB). Where the error lies is in the placement of the active bootable partition within the PIB, if it is not the first entry the bug appears. This is why standard diag tools fail, they read the entries in the PIB, as long as one is marked active and bootable and all the entries correspond logically to the HD's characteristics they say all is OK.

So what you could/should do is boot from A N Other media, use a hex editor to view the MBR and ensure that the active partition is the first entry, (ensure all other entries are replaced and intact) and reboot from the HD.

Cheers.

PJD

-----Original Message-----

From: Kurt Seifried [mailto:bt@seifried.org]

Sent: Wednesday, March 30, 2005 6:36 AM

To: Paul J Docherty; bugs; Bugtraq; secunia

Subject: Re: Portcullis Security Advisory 05-011 ACPI 1.6 BIOS

Does booting from a dos floppy and using "fdisk /mbr" work (or other methods zeroing out the MBR).

Kurt Seifried, kurt@seifried.org

A15B BEE5 B391 B9AD B0EF

AEB0 AD63 0B4E AD56 E574

<http://seifried.org/security/>

----- Original Message -----

## SecurityFocus Bugtraq: RE: Portcullis Security Advisory 05-011 ACPI 1.6 BIOS

From: "Paul J Docherty" <PJD@portcullis-security.com>  
To: "bugs" <bugs@securitytracker.com>; "Bugtraq"  
<bugtraq@securityfocus.com>; "secunia" <vuln@secunia.com>  
Sent: Tuesday, March 29, 2005 5:54 AM  
Subject: Portcullis Security Advisory 05-011 ACPI 1.6 BIOS

Portcullis Security Advisory

Vulnerable System:

This vulnerability affects any workstation running the ACPI 1.6 BIOS implementation.

Vulnerability Title:

BIOS code logic error

Vulnerability discovery and development:

The Portcullis R&D team discovered this vulnerability. Whilst assessing a secured (software access control) laptop environment the team discovered it was possible to cause any system running the vulnerable version of the BIOS to become unstable and no longer boot. Once the coding error was known it could be exploited to cause a near permanent Denial of Service attack.

Affected systems:

The fault was initially found on a Toshiba Satellite Pro A60 running the ACPI BIOS version 1.60. This is a fundamental error that could be exploited in any workstation based on the 1.60 version of the ACPI BIOS. All hard disks, including those encrypted by software or hardware, will be affected. Note that later versions of the ACPI (v1.7 and v1.8), also appear to contain the same coding error however, Portcullis have not tested these versions.

Details:

There is a programming error in the BIOS when the Master Boot Record (MBR) is searched for the bootable disk partition. The error in the BIOS code results in only the first slot in the MBR partition table being tested for the active partition. Where the active partition is not described in the first slot of the MBR table, the BIOS ignores the remaining slots and searches other devices for a boot mechanism, and in consequence fails to start the Operating System.

The BIOS seeks to validate the contents of the MBR and the boot sector in the active partition to achieve confidence in the integrity of the boot mechanism. At various points on the start-up sequence the BIOS reads the MBR from disk and tests the data therein. In at least one case, the BIOS sets out to test all 4 entries in the MBR partition table

RE: Portcullis Security Advisory 05-011 ACPI 1.6 BIOS

but due to treating an absolute pointer as one relative to the start of the MBR, it drops out of the loop after the first iteration. Slots 2, 3 and 4 are never examined and the active partition not found. Specifically, the 512 byte MBR end-of-table is tested by comparing the pointer to see if it has reached end-of-table at 510 bytes. Unfortunately, in the ACPI version the pointer is set to MBR-start plus start-of-table within MBR. Therefore, the pointer begins with a value larger than the size of the MBR. The result is that the first slot fails, when testing for the active partition byte, the test will show an end-of-table result: the subsequent slots are ignored.

An example of the problem is shown when the MBR is read into boot address 0000:7C00h and then tested for an active partition.

```
xor bx, bx ;zero BX

mov es, bx

mov bx, 7C00h ;buffer address ES:BX set to 0000:7C00h

mov cx, 1 ;set sector and cylinder value

xor dh, dh ;and head value to read cylinder 0, head 0, sector 1

mov dl, 80h ;set first hard disk drive

mov ax, 0201h ;set read 1 sector

int 13h ;call BIOS routine to read MBR and assume success

add bx, 446 ;ES:BX point to start of partition table in MBR (BX = 7DBEh)

NextSlot:

    cmp es:[bx], 80h ;is this slot bootable?

    je ActiveOk ;yes, drop out of loop

    add bx, 16 ;increment by length of slot in table
    (BX becomes 7C00h+446+16)

    cmp bx, 510 ;end of slot table reached? error!
    should be cmp bx, 7C00h + 510

    jb NextSlot ;no, look at next entry – branch never taken

    stc ;set no active partition found status

    ret
```

ActiveOk:

```
    clc ;set active partition found status
```

```
ret
```

Impact:

The system will not boot. Standard analysis tools will not identify the contents of the MBR partition as invalid. Unless the help-desk engineer is aware of this BIOS error, he/she will be unable to diagnose the fault. Therefore, the impact is denial of service: the system will not boot and yet there is nothing wrong with the contents of the hard disk.

Exploit:

The error in the BIOS code means that any workstation using this version of the BIOS, can be configured such that the bootable partition is defined below the first slot in the MBR partition table and will not boot. An attack at any time during an operating session can leave the workstation subsequently unable to reboot. The nature of the fault means that it is very difficult to identify and may leave the workstation inoperable for an extended period of time.

Vendor Notified:

Toshiba were notified initially by email, as no response was received this was followed up by telephone on Friday 4-Feb-2005 and again on Wednesday 23-Feb-2005.

Vendor Response:

The A60 laptop works with their supplied configuration. Fault not recognised. Reference supplied by Toshiba is 1-585 92244. When the fault was reported again on 23-Feb-2005 a new fault reference was supplied 1-165 162202 but no technical response was provided by Toshiba.

Workaround/Fix

Either, the BIOS code must be corrected by the manufacturer, or a monitoring device installed to detect any re-configuration that would exploit the vulnerability. Validating and correcting the contents of the MBR at system shutdown is a minimum requirement in these circumstances.

Copyright:

Copyright (c) Portcullis Computer Security Limited 2005. All rights reserved worldwide.

\*\*\*\*\*

The information in this email is confidential and may be

legally privileged. It is intended solely for the addressee.  
Any opinions expressed are those of the individual and do not represent the opinion of the organisation.

Access to this email by persons other than the intended recipient is strictly prohibited.

If you are not the intended recipient, any disclosure, copying, distribution or other action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.

When addressed to our clients any opinions or advice contained in this email is subject to the terms and conditions expressed in the applicable Portcullis Computer Security Limited terms of business.

\*\*\*\*\*