Bug 2957 (CVE-2021-28216) - BootPerformanceTable pointer is read from an NVRAM variable in PEI

Status: RESOLVED FIXED

Alias: CVE-2021-28216

Product: EDK2
Component: Code (show other bugs)
Version: Current
Hardware: All All

Importance: Lowest normal
Assignee: dandanbi

URL:
Keywords:

Depends on:
Blocks:

Reported: 2020-09-09 19:36 UTC by John Mathews
Modified: 2021-11-12 02:53 UTC (History)
CC List: 11 users (show)

See Also:
Branch URL:
Release(s) the issue is observed: EDK II Master
The OS the target platform is running: ---
Package: MdeModulePkg
Release(s) the issues must be fixed: EDK II Master

Attachments	
CVE .json file (904 bytes, application/json) 2021-03-03 11:50 UTC, kevinj	Details
Fix patch based on the latest trunk (69.32 KB, application/octet-stream) 2021-07-22 09:21 UTC, dandanbi	Details
CVE .json file v2 (1.95 KB, application/json) 2021-08-03 15:48 UTC, kevinj	Details
V2 patch (51.91 KB, application/octet-stream) 2021-08-11 21:52 UTC, dandanbi	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

John Mathews 2020-09-09 19:36:28 UTC Description

See the code here:
https://github.com/tianocore/edk2/blob/master/MdeModulePkg/Universal/Acpi/FirmwarePerformanceDataTablePei/FirmwarePerformancePei.c#L149

In the function FpdtStatusCodeListenerPei(), the pointer BootPerformanceTable is read directly from an NVRAM variable ("FirmwarePerformance"). Memory is then updated at that address.
A local attacker may modify the variable at his will, and after reboot the vulnerable code will update memory at the attacker-supplied address.

Should we be locking the FirmwarePerformance variable?

John Mathews 2020-10-08 10:44:55 UTC Comment 1

Moving status to 'confirmed', based on discussion in the 10/7 Infosec mtg.

arose 2021-02-08 18:06:06 UTC Comment 2

Hi, when is this issue targeted to be fixed? Thanks

kevinj 2021-03-03 11:50:21 UTC Comment 3

Created attachment 662 [details]
CVE .json file

I have attached the .json file for CVE classification. Please review and provide feedback.

John Mathews 2021-03-03 13:04:33 UTC Comment 4

(In reply to arose from comment #2)
> Hi, when is this issue targeted to be fixed? Thanks

Hi,
We are looking for someone from community to take ownership and prepare a patch. Currently there is no assigned owner. Would Nvidia be interested in submitting a patch?

John Mathews 2021-03-03 13:04:47 UTC Comment 5

Attacking before EndOfDxe is invalid, but attacking between EndOfDxe and ExitBootServices is valid. Locking the variable could be a solution.

kevinj 2021-03-12 16:02:32 UTC Comment 6

A CVE-ID has been assigned to this bug. Please review the .json file again, especially the version this bug is observed in and inform me when you plan to publicly disclose this bug, so we know when to submit this CVE back to MITRE. Thank you!

kevinj 2021-03-12 16:06:06 UTC Comment 7

A CVE-ID has been assigned to this bug. Please review the .json file again, especially the version this bug is observed in and inform me when you plan to publicly disclose this bug, so we know when to submit this CVE back to MITRE. Thank you!

arose 2021-03-12 17:03:32 UTC Comment 8

Hi, we aren't able to submit a patch, but would like to have proper coordinated disclosure for the bug to be addressed before publicly disclosing. Are there plans for fixing this soon? thanks.

Vincent Zimmer 2021-06-04 12:46:27 UTC Comment 9

For https://www.blackhat.com/us-21/briefings/schedule/index.html#safeguarding-uefi-ecosystem-firmware-supply-chain-is-hardcoded-23685

Does comment “Some issues related to Intel EDKII (reported to Intel in September 2020).” from that link refer to this bug?

Vincent Zimmer 2021-06-04 15:54:01 UTC Comment 10

How about in

https://github.com/tianocore/edk2/blob/master/MdeModulePkg/Universal/Acpi/FirmwarePerformanceDataTableDxe/FirmwarePerformanceDxe.c

after line

```
  //
  // Save Runtime Performance Table pointers to Variable.
  // Don't check SetVariable return status. It doesn't impact FPDT table
generation.
  //
  gRT->SetVariable (
        EFI_FIRMWARE_PERFORMANCE_VARIABLE_NAME,
        &gEfiFirmwarePerformanceGuid,
        EFI_VARIABLE_NON_VOLATILE | EFI_VARIABLE_BOOTSERVICE_ACCESS,
        sizeof (PerformanceVariable),
        &PerformanceVariable
        );
```

we add

```
  EDKII_VARIABLE_LOCK_PROTOCOL  *VariableLock;

  VariableLock = NULL;
  Status = gBS->LocateProtocol(
      &gEdkiiVariableLockProtocolGuid,
      NULL,
      (VOID **)&VariableLock
  );

  if (EFI_ERROR(Status) || VariableLock == NULL) {
     DEBUG((DEBUG_ERROR, "FpdtDxe(%s): Failed to locate Variable Lock Protocol
(%r).\n", mImageIdName, Status));
     return Status;
  }

  Status = VariableLock->RequestToLock(
      VariableLock,
      EFI_FIRMWARE_PERFORMANCE_VARIABLE_NAME,
      &gEfiFirmwarePerformanceGuid
  );

  if (!EFI_ERROR(Status)) {
    DEBUG((DEBUG_ERROR, "FpdtDxe(%s): Failed to lock (%r).\n", mImageIdName,
Status));
    return Status;
  }
```

Bret Barkelew 2021-06-10 19:15:07 UTC Comment 11

We should do this with policies rather than VariableLock, since VariableLock will be deprecated soon.

Vincent Zimmer 2021-06-15 10:46:52 UTC Comment 12

given the history of this feature https://edk2-docs.gitbook.io/security-advisory/overwrite_from_firmwareperformance_variable, maybe there should be a test around protecting this asset, too?

Jeremiah Cox 2021-06-15 14:42:13 UTC Comment 13

S3 is on its way out. S3 performance is not a priority. Could this be removed, or disabled by default?

arose 2021-06-21 15:21:56 UTC Comment 14

Is this issue able to be addressed before BH 2021?

Jeremiah Cox 2021-06-22 15:52:11 UTC Comment 15

@Vincent and @Bret

The variable in question is created in DXE with attributes NV+BS (note that RT is present). Thus a successful attack requires an attacker to have already compromised SMM or bypassed UEFI Secure Boot (to bypass the attribute check).

Reference:
https://github.com/tianocore/edk2/blob/0ecdcb6142037dd1cdd08660a2349960bcf0270a/MdeModulePkg/Universal/Acpi/FirmwarePerformanceDataTableDxe/FirmwarePerformanceDxe.c#L367

This appears to be a non-issue when gEfiMdeModulePkgTokenSpaceGuid.PcdFirmwarePerformanceDataTableS3Support is set to FALSE (the vulnerable FPDT code for S3 is skipped).

I agree with Bret, VariablePolicy is preferred, as it allows us to pin sizes and attributes also (as defense in depth), though backports may need to use VariableLock.

Vincent Zimmer 2021-06-22 18:30:40 UTC Comment 16

speaking of reducing the attack surface, does anyone on the list know why this has to be runtime accessible? would NV+BS suffice?

Vincent Zimmer 2021-06-22 18:33:16 UTC Comment 17

dandan:
It looks like you did some pretty significant updates to this component in the past. Can you create a patch and ensure that there are no functionality regressions? If not, please suggest an alternate person.
thanks

jiewen.yao 2021-06-22 20:48:20 UTC Comment 18

Talked with Dandan. Confirmed she will fix it.

Vincent Zimmer 2021-06-22 21:12:57 UTC Comment 19

thanks Jiewen

Jeremiah Cox 2021-06-24 16:53:52 UTC Comment 20

NVidia confirms this is the 1 (singular) and only EDK2 vulnerability to be disclosed at BlackHat 2021:
https://www.blackhat.com/us-21/briefings/schedule/index.html#safeguarding-uefi-ecosystem-firmware-supply-chain-is-hardcoded-23685

jiewen.yao 2021-06-28 22:52:13 UTC Comment 21

Synced with Dandan.

It is easy to add Lock for this variable. That should happen in EndOdDxe.
Current variable is created at ReadyToBoot.

If we need lock, then we need ReadyToBoot move EndOfDxe.

An extra problem we will handle is to preserve some memory to hold the performance data since EndOfDxe to ReadyToBoot.

Dandan will collect data on a typical server and client, to see how many memory will be preserved.

dandanbi 2021-06-29 01:10:29 UTC Comment 22

Collecting perf data on Server and Client platforms now.
Will provide the final fix after data analysis.

dandanbi 2021-07-02 03:57:11 UTC Comment 23

1. Following are the Perf data size collected on Client and Server platforms:

Perf Data (Bytes)	EndOfDxe	ReadyToBoot	Delta (EndOfDxe->ReadyToBoot)
Platform 1	0x1D9E4	0x2BE0A	0xE426
Platform 2	0x123CE	0x1FEE4	0xDB16

2. Plan to do:

a. Allocate performance data table at EndOfDxe and then lock the varible which store the table address at EndOfDxe.

b. Enlarge PCD gEfiMdeModulePkgTokenSpaceGuid.PcdExtFpdtBootRecordPadSize from 0x20000 to 0x30000 in order to hold the Delta performance data between EndOfDxe and ReadyToBoot.

c. SMM performance data is collected by DXE modules through SMM communication at ReadyToBoot now.
Plan to do SMM communication twice, one for allocating the performance table at EndOfDxe, another is at ReadyToBoot to get SMM performance data between EndOfDxe and ReadyToBoot.

If you have any comment, please let me know.

Jeremiah Cox 2021-07-07 13:55:10 UTC Comment 24

Short-term I would advise setting PcdFirmwarePerformanceDataTableS3Support to FALSE. Long term, feel free to remove the code that adds S3 records to ACPI and FPDT.

Vincent Zimmer 2021-07-07 14:01:38 UTC Comment 25

7/7/2021 infosec meeting feedback:

Recommend "PcdFirmwarePerformanceDataTableS3Support to FALSE" to the system firmware implementation community.

Kevin @ AMI - please update the .json with that statement.

All - please review attached json and subsequent posting w/ the above language

Kevin @ AMI - please submit the CVE to Mitre for publication in order to be public no later than 8/4/2021 in order to be referenced by https://www.blackhat.com/us-21/briefings/schedule/index.html#safeguarding-uefi-ecosystem-firmware-supply-chain-is-hardcoded-23685 presentation on that day.

If Mitre typically takes 2 weeks to process a CVE request, keep that in mind everyone on the content curation and review.

Next infosec meeting is 8/4/21 so any further oppty to discuss this item should be done as part of this ticket.

Given the 'disable' recommendation, the long-term fix proposed by Dandan should not be a gating criteria for CVE publication and information dissemination on this topic.

Thanks again for everyone's input on this topic and Kevin for CVE creation.

Vincent Zimmer 2021-07-21 12:07:16 UTC Comment 26

Kevin @ AMI - any update? Has this been submitted to Mitre?

dandanbi 2021-07-22 09:21:44 UTC Comment 27

Created attachment 774 [details]
Fix patch based on the latest trunk

Attach the fix patch based on the latest trunk for review firstly.

dandanbi 2021-07-26 04:15:51 UTC Comment 28

Hi Jiewen, Jian and Hao,

Could you help review the attached patch?

Thanks,
Dandan

kevinj 2021-08-03 15:48:37 UTC Comment 29

Created attachment 785 [details]
CVE .json file v2

kevinj 2021-08-03 15:50:58 UTC Comment 30

(In reply to Vincent Zimmer from comment #26)
> Kevin @ AMI - any update? Has this been submitted to Mitre?

Vincent, sorry for the delay. I have updated the .json file as requested. I have submitted to Mitre for publication, however not in enough time to be available for the Black Hat briefing. Sorry about that.

Vincent Zimmer 2021-08-04 23:42:20 UTC Comment 31

thanks Kevin

As discussed in today's infosec mtg, even though the CVE isn't live, the details of the issue are public. See https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Safeguarding-UEFI-Ecosystem-Firmware-Supply-Chain-Is-Hardcoded.pdf starting on page 47. As such, the decision in the meeting was to open the bugzilla up to be public so that others can assess the details of the patch.

kevinj 2021-08-05 18:56:09 UTC Comment 32

(In reply to Vincent Zimmer from comment #31)

> thanks Kevin
>
> As discussed in today's infosec mtg, even though the CVE isn't live, the details of the issue are public. See https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Safeguarding-UEFI-Ecosystem-Firmware-Supply-Chain-Is-Hardcoded.pdf starting on page 47. As such, the decision in the meeting was to open the bugzilla up to be public so that others can assess the details of the patch.

Message from MITRE on 8/5/2021 4:46pm below:

"Hello,

Regarding your CVE service request, we have the following question or update:
Expect CVE-2021-28216 to be updated/populated on http://cve.mitre.org in the next few hours. "

Regards,
Kevin Jones

kevinj 2021-08-05 18:58:35 UTC Comment 33

I just checked the MITRE site. The CVE has been populated, thus made public. Link is below.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-28216

Regards,
Kevin Jones

dandanbi 2021-08-11 21:52:57 UTC Comment 34

Created attachment 794 [details]
V2 patch

dandanbi 2021-08-11 21:54:48 UTC Comment 35

As the bug is open, could we send the patch to edk2 community for review?

kevinj 2021-09-29 14:06:04 UTC Comment 36

Has the EDK2 community reviewed this patch?

dandanbi 2021-10-10 23:52:51 UTC Comment 37

(In reply to kevinj from comment #36)
> Has the EDK2 community reviewed this patch?

Patch is under community review now.
https://edk2.groups.io/g/devel/message/81743

kevinj 2021-11-11 19:15:41 UTC Comment 38

Has the EDKII team finished reviewing the patch? If so, has it been pushed to the EDKII master?

dandanbi 2021-11-12 02:53:29 UTC Comment 39

Pushed to edk2 master via
https://github.com/tianocore/edk2/commit/466ebdd2e0919c1538d03cd59833704bd5e1c028