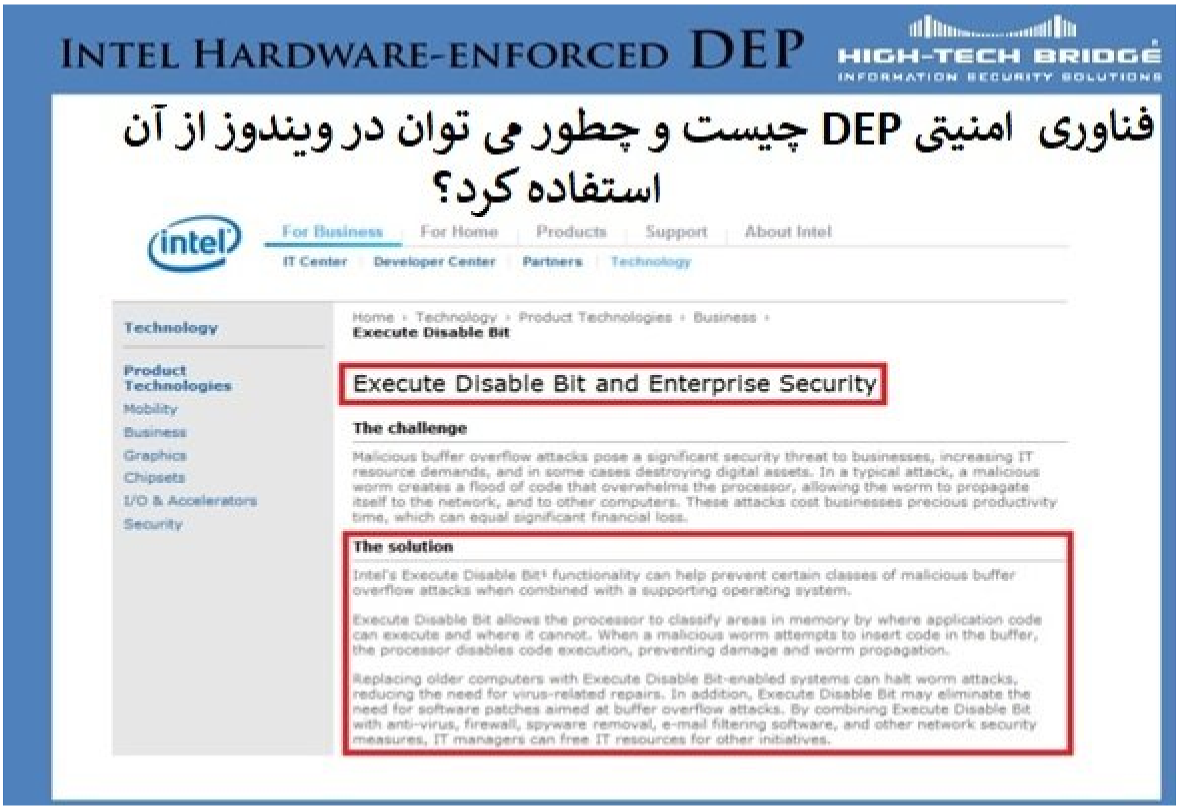
禪

[illegible]

[illegible]


INTEL HARDWARE-ENFORCED DEP

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

فناوری امنیتی DEP چیست و چطور می توان در ویندوز از آن استفاده کرد؟

Execute Disable Bit and Enterprise Security

The challenge

Malicious buffer overflow attacks pose a significant security threat to businesses, increasing IT resource demands, and in some cases destroying digital assets. In a typical attack, a malicious worm creates a flood of code that overwhelms the processor, allowing the worm to propagate itself to the network, and to other computers. These attacks cost businesses precious productivity time, which can equal significant financial loss.

The solution

Intel's Execute Disable Bit¹ functionality can help prevent certain classes of malicious buffer overflow attacks when combined with a supporting operating system.

Execute Disable Bit allows the processor to classify areas in memory by where application code can execute and where it cannot. When a malicious worm attempts to insert code in the buffer, the processor disables code execution, preventing damage and worm propagation.

Replacing older computers with Execute Disable Bit-enabled systems can halt worm attacks, reducing the need for virus-related repairs. In addition, Execute Disable Bit may eliminate the need for software patches aimed at buffer overflow attacks. By combining Execute Disable Bit with anti-virus, firewall, spyware removal, e-mail filtering software, and other network security measures, IT managers can free IT resources for other initiatives.

[illegible] Data Execution [illegible] (DEP) [illegible]
Prevention [illegible].

[illegible]

DEP [illegible] Trojan.Ransomcrypt.K [illegible]

[illegible] (Exception) [illegible]

Access_Violation [illegible]

[illegible] Data Execution Prevention

[illegible] DEP [illegible] DEP [illegible]

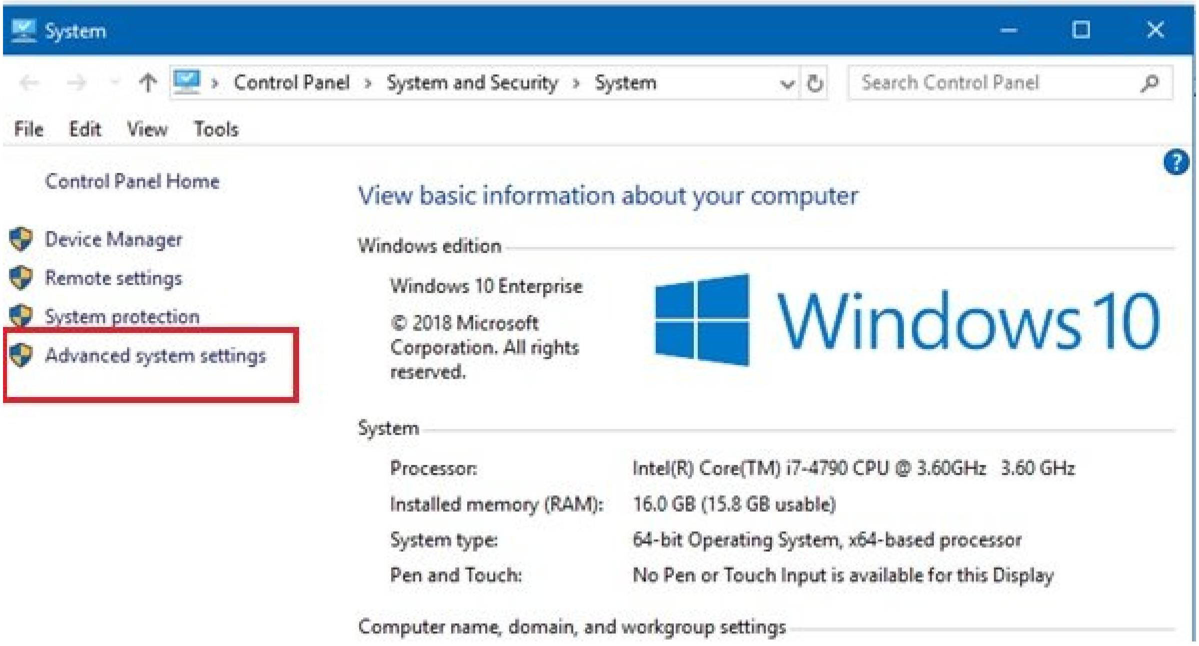
[illegible] DEP [illegible] DEP [illegible]

[illegible]

[illegible]

1. [illegible] 10 [illegible] This PC [illegible] Properties [illegible]

2. [illegible] Advanced system settings [illegible]



View basic information about your computer

Windows edition

Windows 10 Enterprise

© 2018 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 3.60 GHz

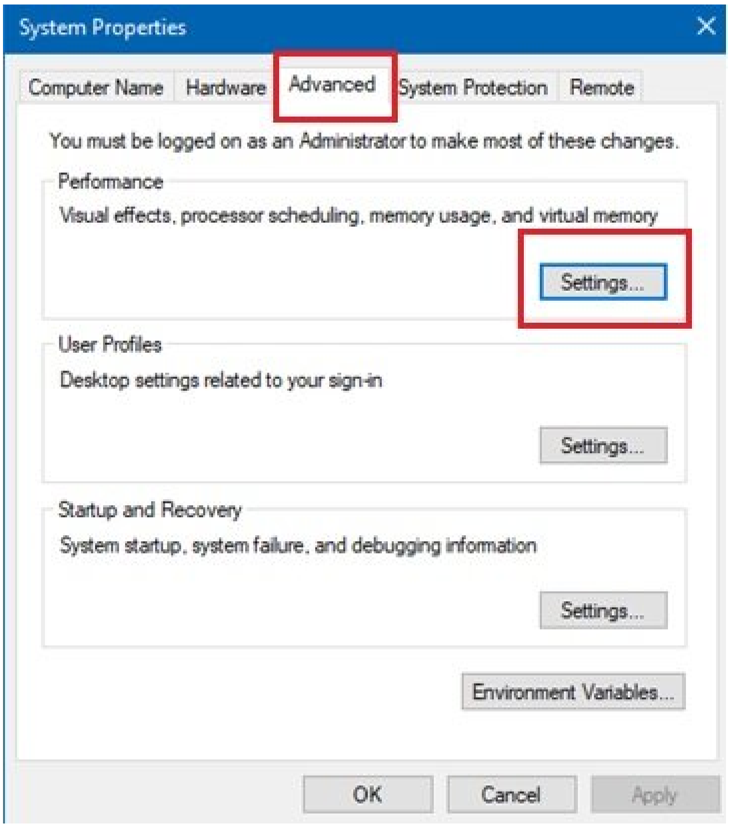
Installed memory (RAM): 16.0 GB (15.8 GB usable)

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

3. [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] Advanced [illegible] [illegible].



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

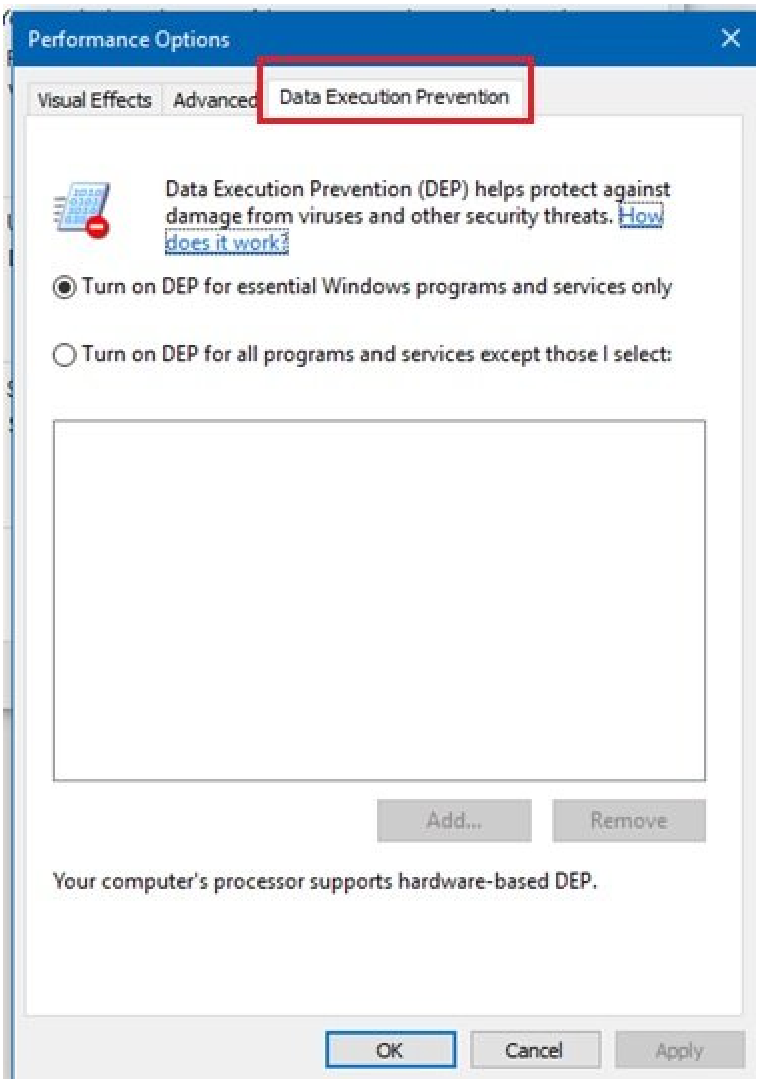
Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. [illegible] [illegible] Performance [illegible] [illegible] [illegible] [illegible] setting [illegible] Performance Options [illegible] [illegible].

5. [illegible] [illegible] [illegible] [illegible] Data Execution Prevention [illegible] [illegible].



Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

● Turn on DEP for essential Windows programs and services only

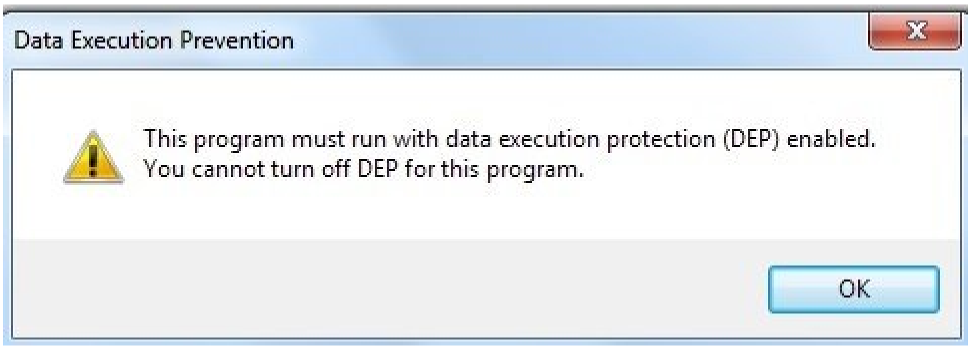
○ Turn on DEP for all programs and services except those I select:

Your computer's processor supports hardware-based DEP.

6. [illegible] DEP [illegible] DEP [illegible].

[illegible] DEP

[illegible] DEP [illegible] DEP [illegible] Turn on DEP for all programs and services except those I select [illegible] Add [illegible] DEP [illegible] Remove [illegible] DEP [illegible].



This program must run with data execution protection (DEP) enabled. You cannot turn off DEP for this program.

[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] DEP [illegible] [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] DEP [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible].

[illegible]:
[illegible] [illegible]
[illegible] [illegible]:
[illegible]
[illegible]
[illegible] [illegible]:
10:15 - 17/05/1397
[illegible]:
[illegible] [illegible] [illegible] [illegible] - [illegible] [illegible] [illegible] - [illegible] [illegible] [illegible] [illegible] - Data Execution Prevention - [illegible] [illegible] [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/13557/%D9%81%D9%86%D8%A7%D9%88%D8%B1%DB%8C-%D9%85%D9%85%D8%A7%D9%86%D8%B9%D8%AA-%D8%A7%D8%B2-%D8%A7%D8%AC%D8%B1%D8%A7%DB%8C-%D8%AF%D8%A7%D8%AF%D9%87%E2%80%8C%D9%87%D8%A7-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%81%D8%B9%D8%A7%D9%84-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D8%AF%D8%9F