Secunia Advisory ID	SA80843
Title	Microsoft Multiple Products Multiple Vulnerabilities
Release date	2018-01-04
Last update	2018-01-04
Criticality	- Moderately critical
Impact	Exposure of sensitive information, Security Bypass
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 5.0 , Overall: 3.7 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:U/RL:OF/RC:C)
CVE references	CVE-2017-5715 | CVE-2017-5753 | CVE-2017-5754 |

Affected operating system and software

Operating systems

Microsoft Windows 10

Microsoft Windows 7

Microsoft Windows 8.1

Microsoft Windows Server 2008

Microsoft Windows Server 2012

Microsoft Windows Server 2016

Software

Microsoft Edge

Microsoft Internet Explorer 11.x

Microsoft SQL Server 2016

Advisory Details:

Description:

Multiple vulnerabilities have been reported in multiple Microsoft products, which can be exploited by malicious, local users to disclose potentially sensitive information and by malicious people to bypass certain security restrictions.

1) An error related to branch prediction during speculative executions in the processor can be exploited to bypass bounds checks and subsequently disclose otherwise restricted kernel memory content via cache side-channel attacks.

2) Another error related to branch prediction during speculative executions in the processor can be exploited to disclose otherwise restricted kernel memory content via cache side-channel attacks.

3) An error related to the exception generation during speculative executions in the processor can be exploited to disclose otherwise restricted kernel memory via cache side-channel attacks.

Solution:

Apply update.

Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems (KB4056890):
Internet Explorer 11 on Windows Server 2016 (KB4056890):
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems (KB4056890):
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems (KB4056890):
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems (KB4056890):

Microsoft Edge on Windows Server 2016 (KB4056890):
Windows 10 Version 1607 for 32-bit Systems (KB4056890):
Windows 10 Version 1607 for x64-based Systems (KB4056890):
Windows Server 2016 (KB4056890):
Windows Server 2016 (Server Core installation) (KB4056890):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890

Internet Explorer 11 on Windows 10 for 32-bit Systems (KB4056893):
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems (KB4056893):
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems (KB4056893):
Internet Explorer 11 on Windows 10 for x64-based Systems (KB4056893):
Microsoft Edge on Windows 10 for x64-based Systems (KB4056893):
Microsoft Edge on Windows 10 for 32-bit Systems (KB4056893):
Windows 10 for 32-bit Systems (KB4056893):
Windows 10 for x64-based Systems (KB4056893):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056893

Internet Explorer 11 on Windows Server 2012 R2 (KB4056568):
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (KB4056568):
Internet Explorer 11 on Windows 8.1 for x64-based systems (KB4056568):
Internet Explorer 11 on Windows 8.1 for 32-bit systems (KB4056568):
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 (KB4056568):
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 (KB4056568):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056568

Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems (KB4056892):
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems (KB4056892):
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems (KB4056892):
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems (KB4056892):
Windows 10 Version 1709 for 32-bit Systems (KB4056892):
Windows Server, version 1709 (Server Core Installation) (KB4056892):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056892

Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems (KB4056891):
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems (KB4056891):
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems (KB4056891):
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems (KB4056891):
Windows 10 Version 1703 for 32-bit Systems (KB4056891):
Windows 10 Version 1703 for x64-based Systems (KB4056891):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056891

Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems (KB4056888):
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems (KB4056888):
Windows 10 Version 1511 for 32-bit Systems (KB4056888):
Windows 10 Version 1511 for x64-based Systems (KB4056888):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056888

Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (KB4057118):
https://www.microsoft.com/downloads/details.aspx?familyid=18a6ec6b-4d21-4de7-8aab-faf42971f9cf

Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU) (KB4057119):
https://www.microsoft.com/downloads/details.aspx?familyid=25723638-2f71-4648-b632-efbaf55c2ab6

Microsoft SQL Server 2017 for x64-based Systems (KB4057122):
https://www.microsoft.com/downloads/details.aspx?familyid=7d70f956-d43d-4af6-a4b5-e55ec4cd1234

Microsoft SQL Server 2017 for x64-based Systems (CU) (KB4052987):
https://www.microsoft.com/downloads/details.aspx?familyid=6fa0ef46-2992-4d39-92ed-9f39f23c8d92

Windows 7 for 32-bit Systems Service Pack 1 (KB4056897):
Windows 7 for x64-based Systems Service Pack 1 (KB4056897):
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 (KB4056897):
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (KB4056897):
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (KB4056897):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056897

Windows 8.1 for 32-bit systems (KB4056898):
Windows 8.1 for x64-based systems (KB4056898):
Windows Server 2012 R2 (KB4056898):
Windows Server 2012 R2 (Server Core installation) (KB4056898):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056898

Windows Server 2012 (KB4056899):
Windows Server 2012 (Server Core installation) (KB4056899):
https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056899

Note: Security updates for Windows 10 and Windows Server 2016 are available via e.g. Windows Update or Windows Update Catalog only.

Provided and/or discovered by:

1, 2) Jann Horn, Google Project Zero, Paul Kocher, Daniel Genkin, University of Pennsylvania and University of Maryland, Mike Hamburg, Rambus, Moritz Lipp, Graz University of Technology, and Yuval Yarom, University of Adelaide and Data61
3) Jann Horn, Google Project Zero, Werner Haas and Thomas Prescher, Cyberus Technology, Daniel Gruss, Moritz Lipp, Stefan Mangard, and Michael Schwarz, Graz University of Technology, and Anders Fogh, GDATA Advanced Analytics

Original advisory:

Meltdown:
https://meltdownattack.com/meltdown.pdf
https://meltdownattack.com
https://spectreattack.com
Google Project Zero:
https://googleprojectzero.blogspot.dk/2018/01/reading-privileged-memory-with-side.html
Spectre:
https://spectreattack.com/spectre.pdf
Microsoft (KB4056890, KB4056893, KB4056568, KB4056892, KB4056891, KB4056888, KB4057118, KB4057119, KB4057122, KB4052987, KB4056897, KB4056898, KB4056899):
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180002
GDATA Advanced Analytics:
https://cyber.wtf/2017/07/28/negative-result-reading-kernel-memory-from-user-mode/

Changelog:

2018-01-04: Initial release