绿盟科技安全预警通告

Meltdown 和 Spectre 处理器漏洞威胁处置手册

预警编号	NS-2018-0001
TAG	CPU 特性、跨平台、远程内存泄露；
关注级别	红，影响范围广，企业及个人用户均须要关注，已公开部分 POC。
发布日期	2018-1-9
版本	V1.2

版本更新说明

V1.1

新增了系统漏洞修复建议

新增了 Windows 系统补丁检测方法

V1.2

新增了 Windows 系统补丁检测修复工具说明

一. 漏洞摘要

2018 年 1 月 4 日，国外研究机构披露了”Meltdown”(CVE-2017-5754)和”Spectre”(CVE-2017-5753& CVE-2017-5715)两组 CPU 特性漏洞。

利用 Meltdown 漏洞，低权限用户可以访问内核的内容，获取本地操作系统底层的信息；当用户通过浏览器访问了包含 Spectre 恶意利用程序的网站时，用户的如帐号，密码，邮箱等个人隐私信息可能会被泄漏；在云服务场景中，利用 Spectre 可以突破用户间的隔离，窃取其他用户的数据。

Meltdown

漏洞编号：CVE-2017-5754

Meltdown 打破了用户应用程序和操作系统之间最基本的隔离。 这种攻击允许程序访问其他程序和操作系统的内存，也就是可以读取到敏感的，秘密的信息。Meltdown 漏洞影响几乎所有的 Intel CPU 和部分 ARM CPU。

参考链接：https://meltdownattack.com/

Spectre

漏洞编号：CVE-2017-5715、CVE-2017-5753

Spectre 打破了不同应用程序之间的隔离。它允许攻击者欺骗无错程序（error-free）并使其泄露秘密信息。事实上，最佳实践的安全检查反而会增加攻击面，并可能使应用程序更容易受到 Spectre 的影响。而 Spectre 则影响所有的 Intel CPU 和 AMD CPU，以及主流的 ARM CPU。从个人电脑、服务器、云计算机服务器到移动端的智能手机，都受到这两组硬件漏洞的影响。

参考链接：https://spectreattack.com/

二. 系统漏洞修复

2.1 Windows 系统修复

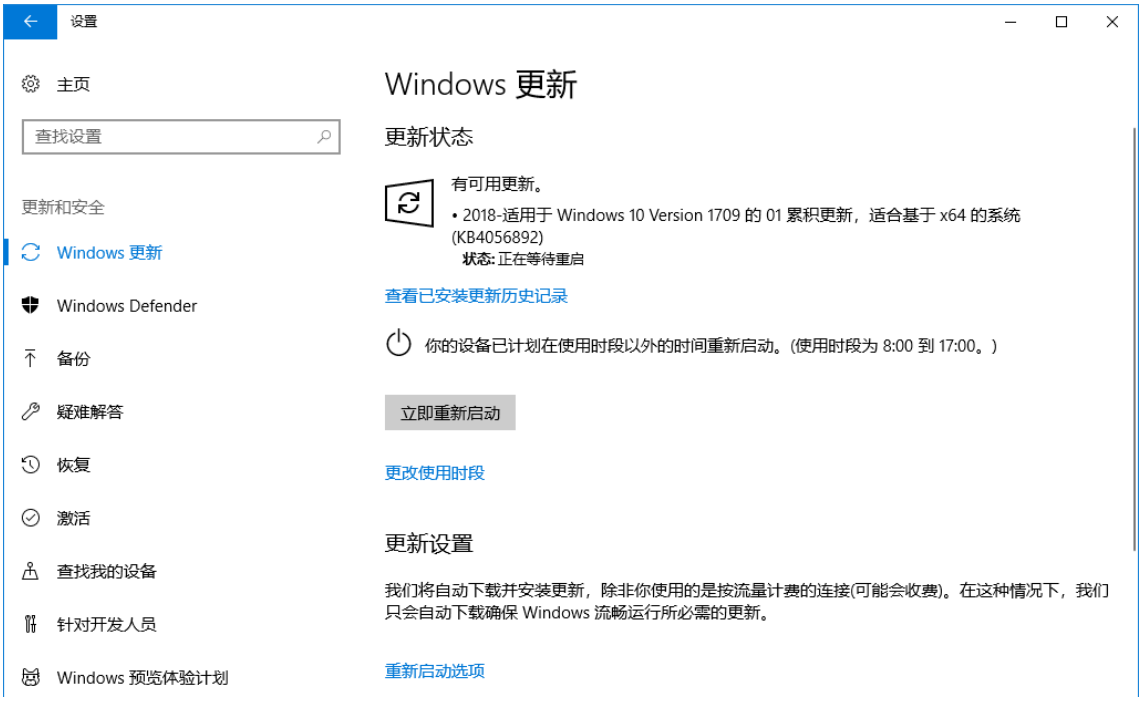
1 月 3 日晚，微软发布了针对 Meltdown 和 Specter 的系统安全更新，企业或个人用户开启系统更新功能及时打全最新的安全补丁。

企业或个人用户可以选择自动更新或手动下载补丁进行更新，补丁下载地址见附录 A。

自动更新：

在企业内网环境中，可以通过 WSUS 服务器连接到 Microsoft Update 来获取更新程序，并分发给企业网络中的客户端计算机实现批量更新。

个人用户可以进入“设置”-“更新与安全”，选择“检查更新”，安装补丁。部分兼容性上存在问题的用户则需要继续耐心等待几天。



手动更新：

根据以下版本与对应 KB 号，在微软安全建议 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002 ，查到对应更新软件包并下载更新。

操作系统版本	对应 KB 号
Windows 10 for 32-bit Systems	KB4056893
Windows 10 for x64-based Systems	KB4056893
Windows 10 Version 1511 for 32-bit Systems	KB4056888
Windows 10 Version 1511 for x64-based Systems	KB4056888
Windows 10 Version 1607 for 32-bit Systems	KB4056890
Windows 10 Version 1607 for x64-based Systems	KB4056890
Windows 10 Version 1703 for 32-bit Systems	KB4056891
Windows 10 Version 1703 for x64-based Systems	KB4056891

Windows 10 Version 1709 for 32-bit Systems	KB4056892
Windows 10 Version 1709 for 64-based Systems	KB4056892
Windows 7 for 32-bit Systems Service Pack 1(Monthly Rollup)	KB4056894
Windows 7 for 32-bit Systems Service Pack 1(Security Only)	KB4056897
Windows 7 for x64-based Systems Service Pack 1(Monthly Rollup)	KB4056894
Windows 7 for x64-based Systems Service Pack 1(Security Only)	KB4056897
Windows 8.1 for 32-bit systems	KB4056898
Windows 8.1 for x64-based systems	KB4056898
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1(Monthly Rollup)	KB4056894
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1(Security Only)	KB4056897
Windows Server 2008 R2 for x64-based Systems Service Pack 1(Monthly Rollup)	KB4056894
Windows Server 2008 R2 for x64-based Systems Service Pack 1(Security Only)	KB4056897
Windows Server 2012 R2	KB4056898
Windows Server 2016	KB4056890

目前的系统补丁尚不能完整修复 Meltdown 和 Spectre 处理器漏洞，企业和用户可能需要额外的芯片组固件更新。如果笔记本电脑/台式机/服务器供应商提供了额外的芯片组固件更新，可以从官方站点获取，安装并完成修补程序。

关于芯片组固件更新

Intel 方面在 1 月 4 号发布了新通告表示，将保证 90%的 CPU（近 5 年的）固件更新会在下周结束前全部放出。目前他们已经在和其他合作伙伴进行这些 CPU 更新。初始设备制造商和其他硬件供应商需要将这些固件更新包含在自己的产品更新中。除此之外，该公司重申，固件更新不会造成显著的性能下降，并承诺会随着时间的推移对这些补丁进行测试和优化，以进一步减轻对性能的影响。

2.2 Linux 系统修复

Red hat:

红帽公司已经发布通告，其中列出受到影响的产品及其当前状态。建议内容表明：对于正在运行受影响版本产品的红帽客户，强烈建议用户尽快根据指导清单进行更新。所有受影响产品都应安装修复补丁。

Ret Hat 安全通告地址：

https://access.redhat.com/security/vulnerabilities/speculativeexecution

受到 Meltdown 影响的产品名称

Red Hat Enterprise Linux 7(已更新)

Red Hat Enterprise Linux 6(部分更新)

Red Hat Enterprise Linux 5(待更新)

RHEL Atomic Host(待更新)

Red Hat Enterprise MRG 2 (已更新)

受到 Spectre 影响的产品名称

Red Hat Enterprise Linux 7 (已更新)

Red Hat Enterprise Linux 6 (部分更新)

Red Hat Enterprise Linux 5 (待更新)

RHEL Atomic Host (待更新)

Red Hat Enterprise MRG 2(已更新)

Red Hat Virtualization 3ELS、4(RHEV-H/RHV-H)(已更新)

Red Hat OpenStack v6 (待更新)

Red Hat OpenStack v7 (待更新)

Red Hat OpenStack v8 (待更新)

Red Hat OpenStack v9(待更新)

Red Hat OpenStack v10 (待更新)

Red Hat OpenStack v11 (待更新)

Red Hat OpenStack v12 (待更新)

CentOS:

CentOS 团队近日面向 64 位（x86_64）CentOS 7 在内的多个版本发布内核安全补丁，重点修复了日前爆发的 Meltdown（熔断）和 Spectre（幽灵）两个漏洞。CentOS 7 基于 Red Hat Enterprise Linux 7，本次发布的安全更新是在 Red Hat 近期发布的修复补丁上进行定制优化的。

目前存在问题的软件包括 kernel-3.10.0-693.11.6.el7.x86_64.rpm, kernel-abi-whitelists-3.10.0-693.11.6.el7.noarch.rpm, kernel-debug-3.10.0-693.11.6.el7.x86_64.rpm, kernel-debug-devel-3.10.0-693.11.6.el7.x86_64.rpm, kernel-devel-3.10.0-693.11.6.el7.x86_64.rpm 以及 kernel-doc-3.10.0-693.11.6.el7.noarch.rpm。

此外 kernel-headers-3.10.0-693.11.6.el7.x86_64.rpm, kernel-tools-3.10.0-693.11.6.el7.x86_64.rpm, kernel-tools-libs-3.10.0-693.11.6.el7.x86_64.rpm, kernel-tools-libs-devel-3.10.0-693.11.6.el7.x86_64.rpm, perf-3.10.0-693.11.6.el7.x86_64.rpm 和 python-perf-3.10.0-693.11.6.el7.x86_64.rpm 也需要更新。

参考链接：

CentOS 6 kernel Security Update

https://lists.centos.org/pipermail/centos-announce/2018-January/022701.html

CentOS 7 kernel Security Update

https://lists.centos.org/pipermail/centos-announce/2018-January/022696.html

Debian:

已针对 Meltdown 漏洞提供更新。

参考链接：https://security-tracker.debian.org/tracker/CVE-2017-5754

Ubuntu:

Ubuntu 安全团队的 Dustin Kirkland 表示新款补丁已经过了两个多月的测试，包括 Ubuntu 12.04 ESM (Extended Security Maintenance), Ubuntu 14.04 LTS, Ubuntu 16.04 LTS 和 Ubuntu 17.10 在内所有尚处于支持状态的 Ubuntu 发行版本都会在近期获得更新。

参考链接：https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown

SUSE:

将为所有企业版 SUSE Linux（SLE）提供 Meltdown 与 Spectre 补丁更新。根据官方描述，也将提供 AMD 与 Intel 处理器微程序包的固件与 QEMU / KVM 更新。

目前已提供更新的 SLE 版本如下：

SLES 12 SP3

SLES 12 SP2

SLES 12 SP1-LTSS

SLES 12-LTSS

SLES 11 SP4

SLES 11 SP3-LTSS

SUSE CaaS Platform

参考链接：https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/

Fedora:

已针对 Fedora Linux 操作系统（含 Fedora26、Fedora27 版本）与 Rawhide (内核 4.15 最终测试版本)提供更新补丁包 ，以降低遭到 Meltdown 攻击的危害。

参考链接：https://fedoramagazine.org/protect-fedora-system-meltdown/

三. Windows 系统补丁检测

Windows 用户可以使用 Powershell 来检查是否安装了正确的更新程序，或是否需要额外的固件更新。用户在启动 PowerShell 时，须确保是以管理员权限启动的，以便安装所需的模块。使用下面的 Powershell 命令，将下载并安装 Powershell 模块，用于测试 Meltdown 和 Specter 的缺陷。

```
Install-Module SpeculationControl
```

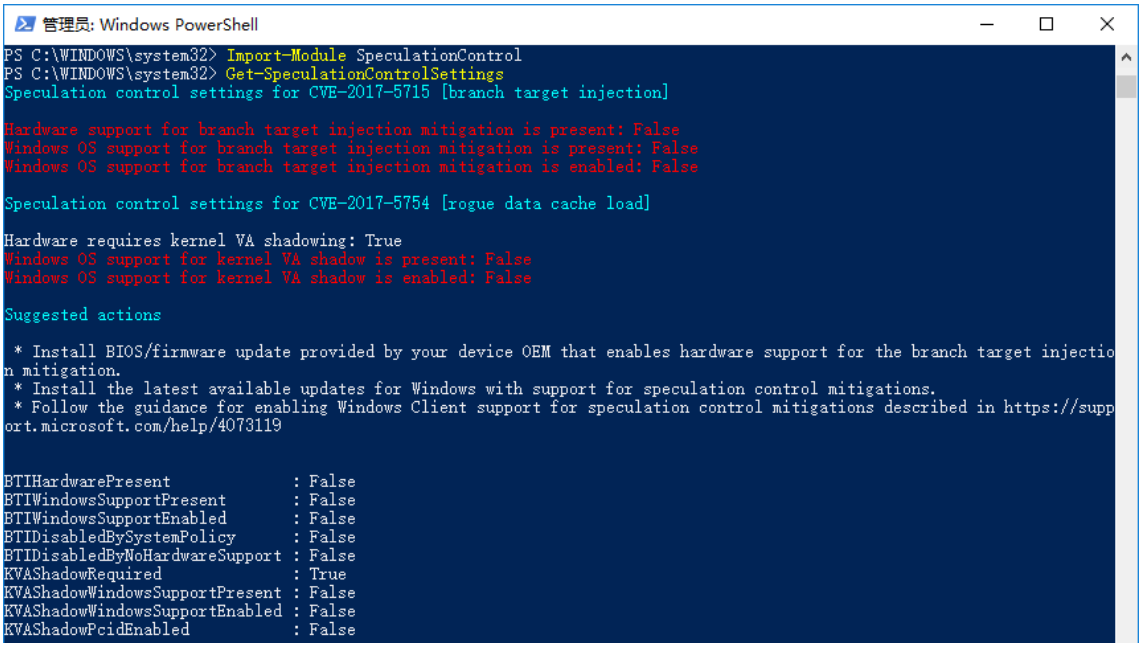
如果用户运行该命令返回的是错误，则可以运行以下命令：

```
Set-ExecutionPolicy Allsigned
```

然后，用户可以运行第二条命令：

```
Get-SpeculationControlSettings
```

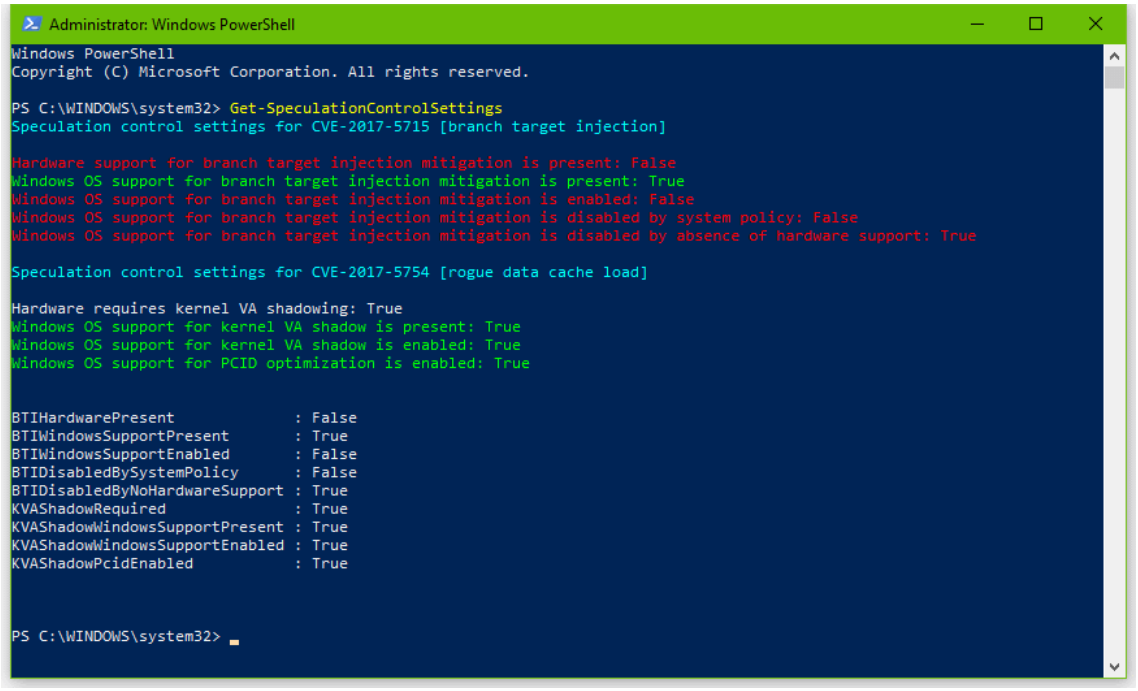
在运行这些命令后看到很多红色的文字，那么可以确认该用户的 CPU 处在威胁之中，如下图。



如检测模块无法执行，可能只有与操作权限的原因导致，开启权限语句：

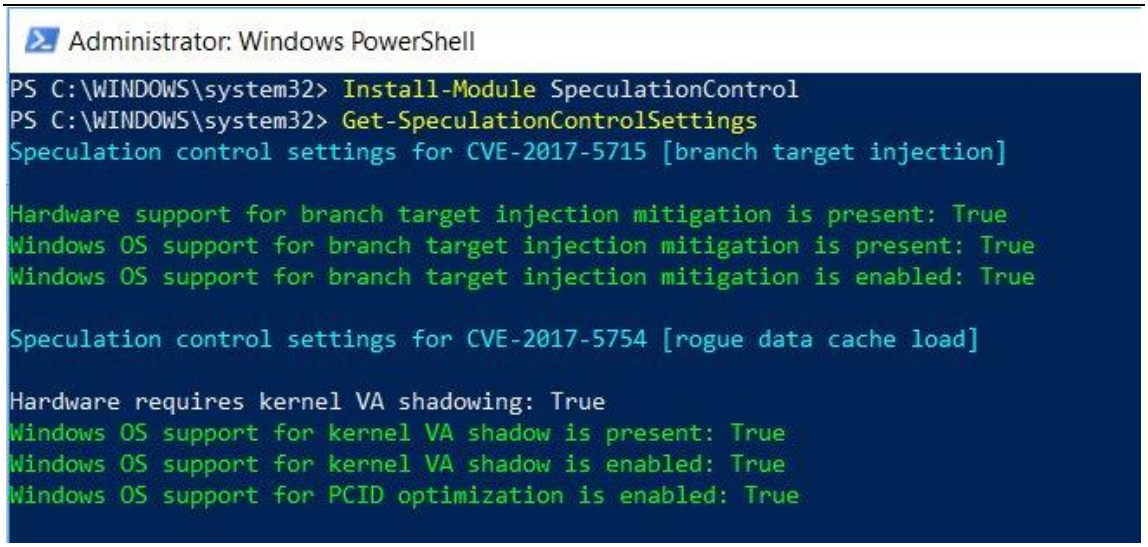
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f
```

在更新补丁后，次运行 Get-SpeculationControlSettings 操作。然后 有两种可能的情况。常见的情况是以下结果：



如图所示表明 Meltdown 补丁已经成功，但是 Spectre 漏洞（CVE-2017-5715）修复不完整。红色的文字内容是指改名用户还是需要额外的芯片组固件更新。如果用户的笔记本电脑/台式机/服务器供应商提供了额外的芯片组固件更新，他们可以从官方站点获取，安装并完成修补程序。

如果一切正常，所有检查将以绿色文本显示，如下所示：



当输出全部为绿色，每个设置都是 True 时，说明已在 Windows 系统级别修复了 Meltdown 和 Spectre 漏洞。

四. Windows Meltdown Spectre 补丁检测工具

目前，部分 Windows 客户可以使用我们编写的漏洞补丁检测工具进行检测和修复，该工具主要功能为检测当前系统是否已经安装补丁，如果未安装会根据系统版本进行提示安装，目前只支持这四个系统版本的自动检测和修复提醒。

【以下所有补丁均由微软官方提供】

Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

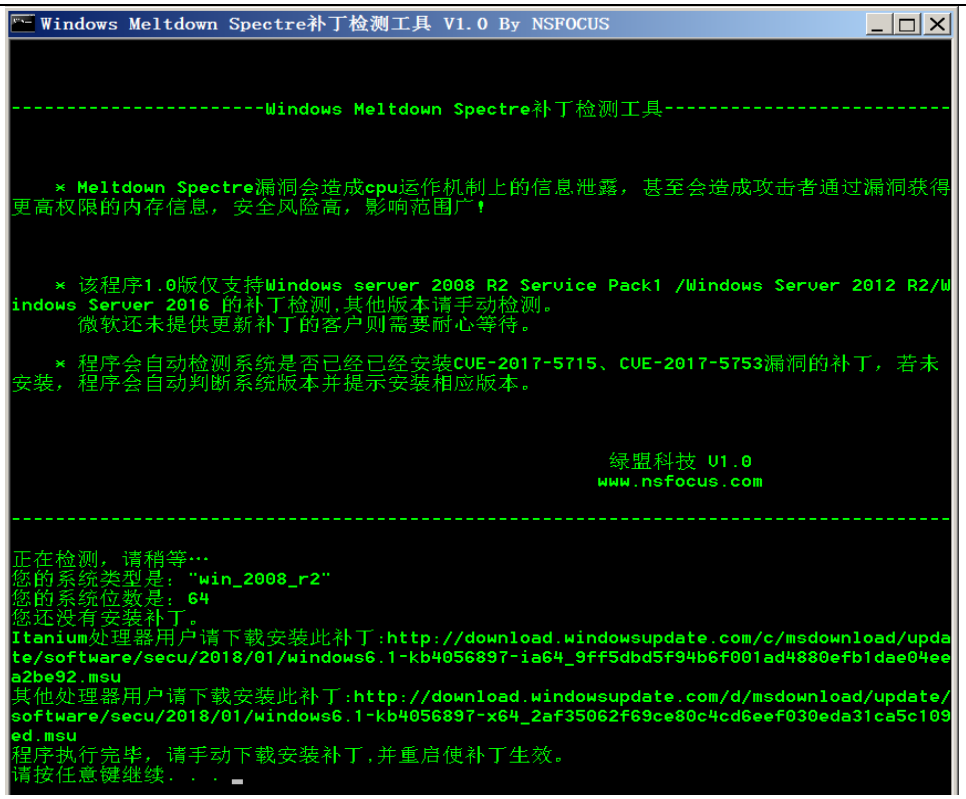
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2012 R2

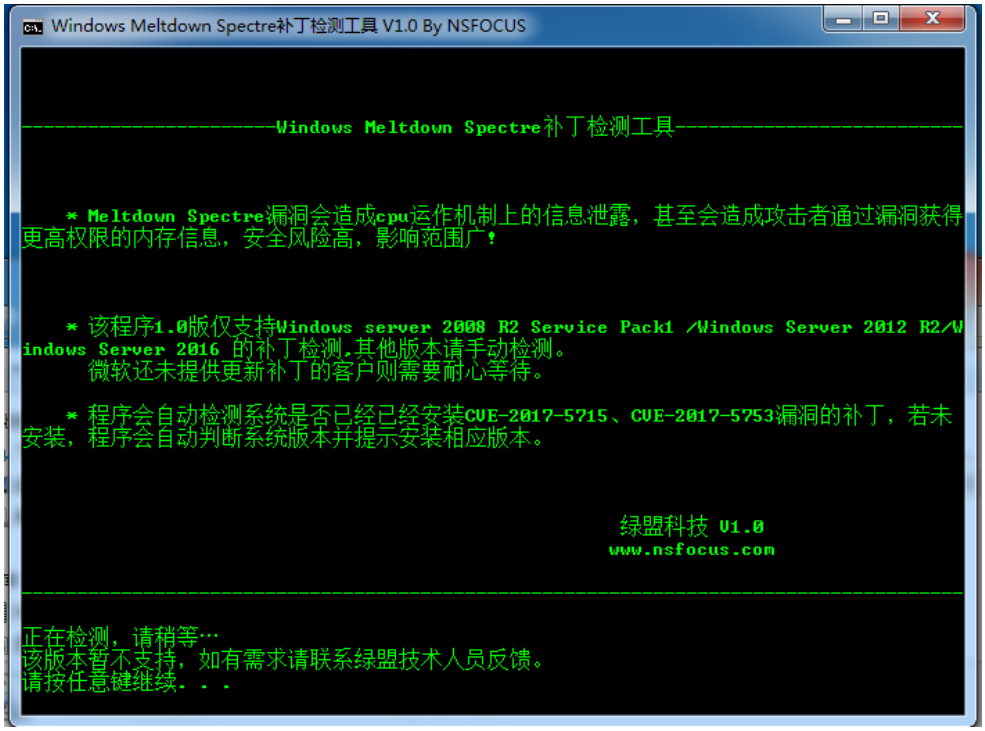
Windows Server 2016

Windows Server 2016 Version 1709

用户通过右键 Windows Meltdown Spectre 补丁检测工具.bat，以管理员权限运行该软件，运行之后，可以看到工具提示正在检测漏洞补丁是否安装。检测完毕之后，如果工具支持该系统版本则会进行下一步的检测并提示补丁下载链接。



如果工具并不支持该系统版本则会进行提示。



用户只需要根据工具提示的链接下载补丁包并进行安装即可，安装后请立即重启使补丁生效。需要注意的是，系统版本为 windows Server 2008 R2 Service Pack 1 的用户在下载补丁包时请务必根据自己的 cpu 型号进行选择。

附录 A Windows 补丁和对应下载列表

操作系统版本	对应 KB 号	补丁下载链接
Windows 10 for 32-bit Systems	KB4056893	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows10.0-kb4056893-x64_d2873bb43413d31871ccb8fea213a96a714a6f87.msu
Windows 10 for x64-based Systems	KB4056893	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056893-x86_b2a28dc6845c85fd32dcd511e3f73f82e46d355f.msu
Windows 10 Version 1511 for 32-bit Systems	KB4056888	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056888-x86_0493b29664aec0bfe7b934479afb45fe83c59cbe.msu
Windows 10 Version 1511 for x64-based Systems	KB4056888	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows10.0-kb4056888-x64_4477b9725a819afd8abc3e5b1f6302361005908d.msu
Windows 10 Version 1607 for 32-bit Systems	KB4056890	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056890-x86_078b34bfdc198bee26c4f13e2e45cb231ba0d843.msu
Windows 10 Version 1607 for x64-based Systems	KB4056890	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056890-x64_1d0f5115833be3d736caeba63c97cfa42cae8c47.msu
Windows 10 Version 1703 for 32-bit Systems	KB4056891	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056891-x86_5e2d98a5cc9d8369a4acd3b3115789a6b1342159.msu
Windows 10 Version 1703 for x64-based Systems	KB4056891	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056891-x64_59726a743b65a221849572757d660f624ed6ca9e.msu

Windows 10 Version 1709 for 32-bit Systems	KB4056892	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows10.0-kb4056892-x86_d3aaf1048d6f314240b8c6fe27932aa52a5e6733.msu
Windows 10 Version 1709 for 64-based Systems	KB4056892	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056892-x64_a41a378cf9ae609152b505c40e691ca1228e28ea.msu
Windows 7 for 32-bit Systems Service Pack 1(Monthly Rollup)	KB4056894	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows6.1-kb4056894-x86_c4ea3ab351b1edb45c0977e0e2e4607b17eeaba7.msu
Windows 7 for 32-bit Systems Service Pack 1(Security Only)	KB4056897	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056897-x86_bb612f57e082c407b8cdad3f4900275833449e71.msu
Windows 7 for x64-based Systems Service Pack 1(Monthly Rollup)	KB4056894	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056894-x64_4ddb21dbf40b3a7c41e17b4bf04242d8b48a5ac3.msu
Windows 7 for x64-based Systems Service Pack 1(Security Only)	KB4056897	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056897-x64_2af35062f69ce80c4cd6eef030eda31ca5c109ed.msu
Windows 8.1 for 32-bit systems	KB4056898	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows8.1-kb4056898-v2-x86_f0781f0b1d96c7b12a18c66f99cf94447b2fa07f.msu
Windows 8.1 for x64-based systems	KB4056898	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows8.1-kb4056898-v2-x64_754f420c1d505f4666437d06ac97175109631bf2.msu
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1(Monthly Rollup)	KB4056894	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056894-ia64_e339ae21a2ee6f1dddcedcdf100367ad7873f78b.msu

Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1(Security Only)	KB4056897	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows6.1-kb4056897-ia64_9ff5dbd5f94b6f001ad4880efb1dae04eea2be92.msu
Windows Server 2008 R2 for x64-based Systems Service Pack 1(Monthly Rollup)	KB4056894	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056894-x64_4ddb21dbf40b3a7c41e17b4bf04242d8b48a5ac3.msu
Windows Server 2008 R2 for x64-based Systems Service Pack 1(Security Only)	KB4056897	http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056897-x64_2af35062f69ce80c4cd6eef030eda31ca5c109ed.msu
Windows Server 2012 R2	KB4056898	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows8.1-kb4056898-v2-x64_754f420c1d505f4666437d06ac97175109631bf2.msu
Windows Server 2016	KB4056890	http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056890-x64_1d0f5115833be3d736caeba63c97cfa42cae8c47.msu

附录 B RedHat 补丁详细信息

产品名称	安装包名称	安全建议	补丁信息
Red Hat Enterprise Linux 7	kernel	RHSA-2018:0007	https://access.redhat.com/errata/RHSA-2018:0007
Red Hat Enterprise Linux 7	kernel-rt	RHSA-2018:0016	https://access.redhat.com/errata/RHSA-2018:0016
Red Hat Enterprise Linux 7	libvirt	RHSA-2018:0029	https://access.redhat.com/errata/RHSA-2018:0029
Red Hat Enterprise Linux 7	qemu-kvm	RHSA-2018:0023	https://access.redhat.com/errata/RHSA-2018:0023

Red Hat Enterprise Linux 7	dracut	RHBA-2018:0042	https://access.redhat.com/errata/RHBA-2018:0042
Red Hat Enterprise Linux 7.3 Extended Update Support**	kernel	RHSA-2018:0009	https://access.redhat.com/errata/RHSA-2018:0009
Red Hat Enterprise Linux 7.3 Extended Update Support**	libvirt	RHSA-2018:0031	https://access.redhat.com/errata/RHSA-2018:0031
Red Hat Enterprise Linux 7.3 Extended Update Support**	qemu-kvm	RHSA-2018:0027	https://access.redhat.com/errata/RHSA-2018:0027
Red Hat Enterprise Linux 7.3 Extended Update Support**	dracut	RHBA-2018:0043	https://access.redhat.com/errata/RHBA-2018:0043
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	kernel	RHSA-2018:0010	https://access.redhat.com/errata/RHSA-2018:0010
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	libvirt	RHSA-2018:0032	https://access.redhat.com/errata/RHSA-2018:0032
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	qemu-kvm	RHSA-2018:0026	https://access.redhat.com/errata/RHSA-2018:0026
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	dracut	待更新	-
Red Hat Enterprise Linux 6	kernel	RHSA-2018:0008	https://access.redhat.com/errata/RHSA-2018:0008
Red Hat Enterprise Linux 6	libvirt	RHSA-2018:0030	https://access.redhat.com/errata/RHSA-2018:0030
Red Hat Enterprise Linux 6	qemu-kvm	RHSA-2018:0024	https://access.redhat.com/errata/RHSA-2018:0024
Red Hat Enterprise Linux 6.7 Extended Update Support**	kernel	RHSA-2018:0011	https://access.redhat.com/errata/RHSA-2018:0011
Red Hat Enterprise Linux 6.7 Extended Update Support**	libvirt	待更新	-

Red Hat Enterprise Linux 6.6 Advanced Update Support***,****	qemu-kvm	待更新	-
Red Hat Enterprise Linux 6.5 Advanced Update Support***	kernel	RHSA-2018:0022	https://access.redhat.com/errata/RHSA-2018:0022
Red Hat Enterprise Linux 6.5 Advanced Update Support***	libvirt	待更新	-
Red Hat Enterprise Linux 6.5 Advanced Update Support***	qemu-kvm	待更新	-
Red Hat Enterprise Linux 6.4 Advanced Update Support***	kernel	RHSA-2018:0018	https://access.redhat.com/errata/RHSA-2018:0018
Red Hat Enterprise Linux 6.4 Advanced Update Support***	libvirt	待更新	-
Red Hat Enterprise Linux 6.4 Advanced Update Support***	qemu-kvm	待更新	-
Red Hat Enterprise Linux 6.2 Advanced Update Support***	kernel	RHSA-2018:0020	https://access.redhat.com/errata/RHSA-2018:0020
Red Hat Enterprise Linux 6.2 Advanced Update Support***	libvirt	待更新	-
Red Hat Enterprise Linux 6.2 Advanced Update Support***	qemu-kvm	待更新	-
Red Hat Enterprise Linux 5 Extended Lifecycle Support*	kernel	待更新	-
Red Hat Enterprise Linux 5 Extended Lifecycle Support*	libvirt	待更新	-
Red Hat Enterprise Linux 5 Extended Lifecycle Support*	qemu-kvm	待更新	-

Red Hat Enterprise Linux 5.9 Advanced Update Support***	kernel	待更新	-
Red Hat Enterprise Linux 5.9 Advanced Update Support***	libvirt	待更新	-
Red Hat Enterprise Linux 5.9 Advanced Update Support***	qemu-kvm	待更新	-
RHEL Atomic Host	kernel	Images respun on 5 January 2018	-
Red Hat Enterprise MRG 2	kernel-rt	RHSA-2018:0021	https://access.redhat.com/errata/RHSA-2018:0021
Red Hat Virtualization 4 (RHEV-H/RHV-H)	redhat-virtualization-host	RHSA-2018:0047	https://access.redhat.com/errata/RHSA-2018:0047
Red Hat Virtualization 4 (RHEV-H/RHV-H)	rhvm-appliance	RHSA-2018:0045	https://access.redhat.com/errata/RHSA-2018:0045
Red Hat Virtualization 4 (RHEV-H/RHV-H)	qemu-kvm-rhev	RHSA-2018:0025	https://access.redhat.com/errata/RHSA-2018:0025
Red Hat Virtualization 4 (RHEV-H/RHV-H)	vdsm	RHSA-2018:0050	https://access.redhat.com/errata/RHSA-2018:0050
Red Hat Virtualization 4 (RHEV-H/RHV-H)	ovirt-guest-agent-docker	RHSA-2018:0047	https://access.redhat.com/errata/RHSA-2018:0047
Red Hat Virtualization 4 (RHEV-H/RHV-H)	rhevm-setup-plugins	RHSA-2018:0051	https://access.redhat.com/errata/RHSA-2018:0051
Red Hat Virtualization 3 (RHEV-H/RHV-H)	redhat-virtualization-host	RHSA-2018:0044	https://access.redhat.com/errata/RHSA-2018:0044
Red Hat OpenStack Platform 8.0 (Liberty)	qemu-kvm-rhev	RHSA-2018:0056	https://access.redhat.com/errata/RHSA-2018:0056
Red Hat OpenStack Platform 8.0 (Liberty)	director images	待更新	-
Red Hat OpenStack Platform 9.0 (Mitaka)	qemu-kvm-rhev	RHSA-2018:0057	https://access.redhat.com/errata/RHSA-2018:0057

Red Hat OpenStack Platform 9.0 (Mitaka)	director images	待更新	-
Red Hat OpenStack Platform 10.0 (Newton)	qemu-kvm-rhev	RHSA-2018:0058	https://access.redhat.com/errata/RHSA-2018:0058
Red Hat OpenStack Platform 10.0 (Newton)	director images	待更新	-
Red Hat OpenStack Platform 11.0 (Ocata)	qemu-kvm-rhev	RHSA-2018:0059	https://access.redhat.com/errata/RHSA-2018:0059
Red Hat OpenStack Platform 11.0 (Ocata)	director images	待更新	-
Red Hat OpenStack Platform 12.0 (Pike)	qemu-kvm-rhev	RHSA-2018:0060	https://access.redhat.com/errata/RHSA-2018:0060
Red Hat OpenStack Platform 12.0 (Pike)	director images	待更新	-
Red Hat OpenStack Platform 12.0 (Pike)	containers	待更新	-