# Meltdown' and 'Spectre' guidance

**Guidance for enterprise administrators in relation to the recently published processor vulnerabilities 'Meltdown' and 'Spectre'**

## What are Meltdown/Spectre?

'Meltdown' and 'Spectre' are two related, side-channel attacks against modern CPU microprocessors that can result in unprivileged code reading data it should not be able to.

Most devices - from smartphones to hardware in data centres - may be vulnerable to some extent. Vendors are working on (or have already released) patches to mitigate the issue. **The NCSC advise you to patch your devices as soon as possible**.

---

## What are the vulnerabilities?

Processors in most devices employ a range of techniques to speed up their operation. The Meltdown and Spectre vulnerabilities allow some of these techniques to be abused, in order to obtain information about areas of memory not normally visible to an attacker. This could include secret keys or other sensitive data.

These vulnerabilities comprise:

- **Spectre** (bounds check bypass and branch target injection): CVE-2017-5753 and CVE-2017-5715
- **Meltdown** (rogue data cache load): CVE-2017-5754

For more information, visit the Spectre attack website: **https://spectreattack.com/**

---

## What is the impact?

In the worst case, code running on a device can access areas of memory it does not have permission to access. This can result in compromise of sensitive data, including secret keys and passwords.

---

## What can I do to protect myself and my organisation?

Device and platform manufacturers are releasing updates to supported products which will mitigate this issue. Ensure that the latest patches have been installed, and that you are not using unsupported devices as these will not be fixed.

The following section summarises responses from the major suppliers that the NCSC is aware of.

### Cloud services

The major cloud service providers are installing fixes on their own platforms. However, in a virtualised environment, fixes are required for both the hypervisor and guest virtual machines. Therefore, when using Infrastructure as a Service (IaaS), you will need to update the operating systems of any virtual machines and container base images that you manage. For Platform as a Service (PaaS) and Software as a Service (SaaS), your provider should install these patches for you. If in doubt, check that your service provider:

- is aware of the issue and installing fixes
- is providing advice for dealing with the issue

### Data centres/servers

Operating systems and hypervisors need patches, as does the firmware of the physical machines you are running. The major equipment manufacturers (OEMs) are producing patches; you should obtain these directly from the OEM. Patches for Linux are also being produced and will be included by the most common distributions. These should be installed as soon as they are available.

### End user devices

The major operating system vendors have produced patches which mitigate the issues, though some parts of the patches need to be installed via the equipment manufacturer (OEM) as they contain platform-specific elements. This means that **it's not sufficient just to update the operating system - you will need to check that the underlying firmware is also up to date**. Links are provided at the end of this page.

### Applications and software

Software compilers need to be updated to protect applications from the Spectre vulnerabilities. Once compilers have been updated, applications will need to be recompiled to take advantage of these mitigations. As with operating systems, applications should be regularly updated to ensure the latest security fixes are applied.

---

## More information

Some CPU microprocessors are affected more than others. Check with your processor's manufacturer to find out the full impact of the vulnerabilities.

This attack requires code to be running on the target device, so is currently a local escalation of privilege attack. However, the vulnerabilities may be exploitable from within application sandboxes (including web browsers), so take care when executing any untrusted code, including JavaScript on web pages.

| | |
|---|---|
| Intel | Security Advisory / Newsroom / Planned microcode updates |
| Microsoft | Security Guidance |
| Amazon | Security Bulletin |
| ARM | Security Update |
| Google | Project Zero Blog |
| Mitre | CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 |
| Red Hat | Vulnerability Response |
| Suse | Vulnerability Response |
| Apple | Vulnerability Response |

## Spectre attack website: **https://spectreattack.com/**

**PUBLISHED**

13 February 2018

**REVIEWED**

13 February 2018

**VERSION**

1.0

**WRITTEN FOR**

Small & medium sized organisations

Large organisations

Cyber security professionals

Public sector