

# Table of Contents

<b>CVE List</b> .....	1
<i>Check for Patches in Kernel</i> .....	1
<b>List of Operating Systems</b> .....	1



# CVE List

- [CVE-2017-5715](#)
  - Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
- [CVE-2017-5753](#)
  - Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
- [CVE-2017-5754](#)
  - Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

## Check for Patches in Kernel

```
grep "cpu_insecure\|cpu_meltdown\|kaiser" /proc/cpuinfo && echo "Patched "
|| echo "Unpatched"
```

## List of Operating Systems

OS	Distro	Release	Spectre Variant 1	Spectre Variant 2	Meltdown	Kernel
Linux	Centos	6	<a href="#">RHSA-2018:0008</a> , <a href="#">RHSA-2018:0013</a> , <a href="#">RHSA-2018:0024</a>	N/A	<a href="#">RHSA-2018:0008</a> , <a href="#">RHSA-2018:0013</a> , <a href="#">RHSA-2018:0024</a>	2.6.32-696.18.7
Linux	Centos	7	<a href="#">Forum</a> , <a href="#">Bugzilla</a>	N/A	<a href="#">Forum</a> , <a href="#">Bugzilla</a>	3.10.0-693.11.6

From:  
<https://esgr.in/wiki/> - **eSGR Documentation**

Permanent link:  
<https://esgr.in/wiki/systems/meltdown-spectre?rev=1515657974>

Last update: **2018/01/11 08:06**

