

Table of Contents

- CVE List** 1
 - Check for Patches in Kernel*** 1
- List of Operating Systems** 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

```
dmesg | grep "cpu_insecure\|cpu_meltdown\|kaiser\|x86/pti" && echo "Patched" || echo "Unpatched"
```

List of Operating Systems

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

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

Permanent link:
<https://esgr.in/wiki/systems/meltdown-spectre?rev=1515658803>

Last update: **2018/01/11 08:20**

