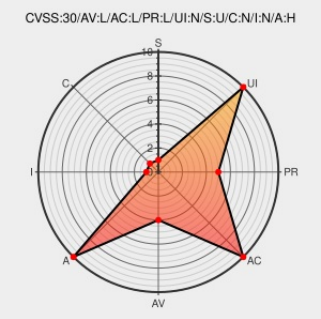
# CVE-2015-2672

Published on: 05/02/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

## CVE-2015-2672

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Linux Kernel from Linux contain the following vulnerability:

The xsave/xrstor implementation in arch/x86/include/asm/xsave.h in the Linux kernel before 3.19.2 creates certain .altinstr_replacement pointers and consequently does not provide any protection against instruction faulting, which allows local users to cause a denial of service (panic) by triggering a fault, as demonstrated by an unaligned memory operand or a non-canonical address memory operand.

CVE-2015-2672 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 4.9 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| | www.kernel.org<br>text/plain | CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.19.2 |

| | | |
|---|---|---|
| kernel/git/torvalds/linux.git - Linux kernel source tree | Vendor Advisory<br>git.kernel.org<br>text/html | CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=06c8173eb92bbfc03a0fe8bb64315857d0badd06 |
| oss-security - Re: CVE Request: Linux kernel unprivileged denial-of-service due to mis-protected xsave/xrstor instructions. | www.openwall.com<br>text/html | MLIST [oss-security] 20150321 Re: CVE Request: Linux kernel unprivileged denial-of-service due to mis-protected xsave/xrstor instructions. |
| 1204729 – (CVE-2015-2672) CVE-2015-2672 kernel: unprivileged denial-of-service due to mis-protected xsave/xrstor instructions | bugzilla.redhat.com<br>text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1204729 |
| x86/fpu/xsaves: Fix improper uses of __ex_table · torvalds/linux@06c8173 · GitHub | Vendor Advisory<br>github.com<br>text/html | CONFIRM github.com/torvalds/linux/commit/06c8173eb92bbfc03a0fe8bb64315857d0badd06 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | All | All | All | All |

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→