



# CVE-2019-19339

Published on: 01/17/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:59 PM UTC

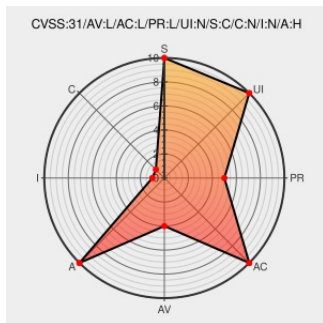
## CVE-2019-19339

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Enterprise Linux](#) from [Redhat](#) contain the following vulnerability:

It was found that the Red Hat Enterprise Linux 8 kpatch update did not include the complete fix for CVE-2018-12207. A flaw was found in the way Intel CPUs handle inconsistency between, virtual to physical memory address translations in CPU's local cache and system software's Paging structure entries. A privileged guest user may use

this flaw to induce a hardware Machine Check Error on the host processor, resulting in a severe DoS scenario by halting the processor. System software like OS OR Virtual Machine Monitor (VMM) use virtual memory system for storing program instructions and data in memory. Virtual Memory system uses Paging structures like Page Tables and Page Directories to manage system memory. The processor's Memory Management Unit (MMU) uses Paging structure entries to translate program's virtual memory addresses to physical memory addresses. The processor stores these address translations into its local cache buffer called - Translation Lookaside Buffer (TLB). TLB has two parts, one for instructions and other for data addresses. System software can modify its Paging structure entries to change address mappings OR certain attributes like page size etc. Upon such Paging structure alterations in memory, system software must invalidate the corresponding address translations in the processor's TLB cache. But before this TLB invalidation takes place, a privileged guest user may trigger an instruction fetch operation, which could use an already cached, but now invalid, virtual to physical address translation from Instruction TLB (ITLB). Thus accessing an invalid physical memory address and resulting in halting the processor due to the Machine Check Error (MCE) on Page Size Change.

CVE-2019-19339 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Red Hat** - **kpatch**: version = n/a

CVSS3 Score: **6.5 - MEDIUM**

Attack  
Vector

Attack  
Complexity

Privileges  
Required

User  
Interaction

| CVE References                                                                          |                                                                                                          |                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                                                             | Tags                                                                                                     | Link                                                                                                                                                                 |
| 1782199 – (CVE-2019-19339) CVE-2019-19339 kpatch: hw: incomplete fix for CVE-2018-12207 | <div>Issue Tracking</div> <div>Vendor Advisory</div> <div>bugzilla.redhat.com</div> <div>text/html</div> | <div> CONFIRM</div> <div>bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-19339</div> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

| Type                                                 | Vendor | Product              | Version | Update | Edition | Language |
|------------------------------------------------------|--------|----------------------|---------|--------|---------|----------|
| Operating System                                     | Redhat | Enterprise Linux     | 8.0     | All    | All     | All      |
| Operating System                                     | Redhat | Enterprise Linux     | 8.0     | All    | All     | All      |
| Operating System                                     | Redhat | Enterprise Linux Eus | 8.1     | All    | All     | All      |
| Operating System                                     | Redhat | Enterprise Linux Eus | 8.1     | All    | All     | All      |
| cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:     |        |                      |         |        |         |          |
| cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:     |        |                      |         |        |         |          |
| cpe:2.3:o:redhat:enterprise_linux_eus:8.1:*:*:*:*:*: |        |                      |         |        |         |          |
| cpe:2.3:o:redhat:enterprise_linux_eus:8.1:*:*:*:*:*: |        |                      |         |        |         |          |

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)