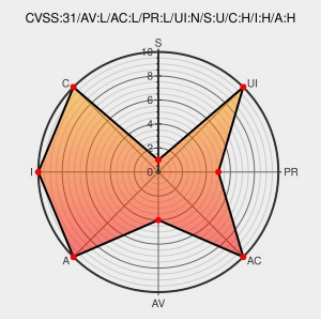
# CVE-2017-17857

Published on: 12/22/2017 12:00:00 AM UTC

Last Modified on: 02/07/2023 10:17:00 PM UTC

## CVE-2017-17857

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




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

The check_stack_boundary function in kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging mishandling of invalid variable stack read operations.

CVE-2017-17857 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.8 - HIGH

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

### CVSS2 Score: 7.2 - HIGH

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| kernel/git/torvalds/linux.git - Linux kernel source tree | Vendor Advisory, git.kernel.org, text/html | MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ea25f914dc164c8d56b36147ecc86bc65f83c469 |
| oss-security - Linux >=4.9: eBPF | Mailing List | MISC www.openwall.com/lists/oss-security/2017/12/21/2 |

| | | |
|---|---|---|
| memory corruption bugs | Third Party Advisory<br>www.openwall.com<br>text/html | |
| bpf: fix missing error return in check_stack_boundary() · torvalds/linux@ea25f91 · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | MISC<br>github.com/torvalds/linux/commit/ea25f914dc164c8d56b36147ecc86bc65f83c469 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→