# CVE Detail – CVE-2020-8835

In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.96065

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-125: Out-of-bounds Read
* CWE-787: Out-of-bounds Write

## CAPEC(s)

* CAPEC-540: Overread Buffers

## Affected Products

* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:linux:linux\_kernel:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:30:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:31:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:18.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:19.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:cloud\_backup:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:hci\_management\_node:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:solidfire:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:steelstore\_cloud\_integrated\_storage:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:a700s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:8300\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:8700\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:a400\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:a320\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:c190\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:a220\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:fas2720\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:fas2750\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:a800\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h300s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h500s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h700s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h300e\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h500e\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h700e\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h410s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h610c\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h610s\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:netapp:h615c\_firmware:-:\*:\*:\*:\*:\*:\*:\*