Scan Report

February 28, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "centos7_31". The scan started at Mon Feb 28 15:21:08 2022 UTC and ended at Mon Feb 28 15:30:25 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.137.31	8	6	0	0	0
Total: 1	8	6	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 14 results selected by the filtering described above. Before filtering there were 76 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.137.31	SSH	Success	Protocol SSH, Port 22, User root

2 Results per Host

2.1 192.168.137.31

Host scan start	Mon Feb 28 15:23:06 2022 UTC
Host scan end	Mon Feb 28 15:30:21 2022 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary

. . . continues on next page . . .

... continued from previous page ...

This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Source Edition (GSE)
- Greenbone Security Manager TRIAL (formerly Greenbone Community Edition (GCE))
used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result

```
Version of installed component:          21.4.2 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on GVM >= 10)
Latest available openvas-scanner version: 21.4.3
Reference URL(s) for the latest available version: https://community.greenbone.n
↪et/t/gvm-21-04-stable-initial-release-2021-04-16/8942
```

Solution:
Solution type: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method
Details: `Report outdated / end-of-life Scan Engine / Environment (local)`
OID:1.3.6.1.4.1.25623.1.0.108560
Version used: `2022-02-14T00:00:02Z`

References

```
url: https://www.greenbone.net/en/testnow/
url: https://community.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03
↪-07/211
url: https://community.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-0
↪4-05/208
url: https://community.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-1
↪0-14/3674
url: https://community.greenbone.net/t/gvm-20-08-end-of-life-initial-release-202
↪0-08-12/6312
url: https://community.greenbone.net/t/gvm-21-04-stable-initial-release-2021-04-
↪16/8942
url: https://docs.greenbone.net/GSM-Manual/gos-21.04/en/reports.html#creating-an
```

... continues on next page ...

... continued from previous page ...

↪-override

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:3801)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:3801 advisory.

Vulnerability Detection Result
Vulnerable package: kernel
Installed version: kernel-3.10.0-1160.el7
Fixed version: kernel-3.10.0-1160.45.1.el7

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: Improper handling of VM_IO<pipe>VM_PFNMAP vmas in KVM can bypass RO checks (CVE-2021-22543)
kernel: powerpc: KVM guest OS users can cause host OS memory corruption (CVE-2021-37576)
kernel: SVM nested virtualization issue in KVM (AVIC support) (CVE-2021-3653)
kernel: SVM nested virtualization issue in KVM (VMLOAD/VMSAVE) (CVE-2021-3656)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):
Kernel panic due to double fault with DLM reporting for socket error 'sk_err=32/0' (BZ#1834878)
'MFW indication via attention' message getting logged frequently after every 5 minutes (BZ#1854544)
lpfc fails to discovery in pt2pt with '2754 PRLI failure DID:0000EF Status:x9/x91e00, data: x0' (BZ#1922479)
pcpu_get_vm_areas using most memory from VmallocUsed (BZ#1970618)
RHEL 7.9.z [qedf driver] Racing condition between qedf_cleanup_fcport and releasing command Azure after timeout (BZ#1982702)Azure>
RHEL 7.9 reports GPU/IB topology incorrectly on some Azure SKUs (BZ#1984128)stable gueststable guest ABI ABI>
Hot add CPU after migration cause guest hang (BZ#1991856)
i40e driver crash at RIP: i40e_config_vf_promiscuous_mode+0x165 (BZ#1993850)nfs> nfs
Performance issue since commit 5a4f6f11951e (BZ#1995649)kernel> kernel
Indefinite waiting for RCU callback while removing cgroup (BZ#2000973)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:3801)`
OID:1.3.6.1.4.1.25623.1.0.883383
Version used: `2021-11-29T00:00:10Z`

References
`cve: CVE-2021-3653`
`cve: CVE-2021-3656`
`cve: CVE-2021-22543`
`cve: CVE-2021-37576`
`advisory-id: CESA-2021:3801`
`url: https://lists.centos.org/pipermail/centos-announce/2021-November/048398.htm`
`↪l`
`cert-bund: CB-K21/0879`
`cert-bund: CB-K21/0849`
`cert-bund: CB-K21/0808`
`cert-bund: CB-K21/0696`
`dfn-cert: DFN-CERT-2022-0074`
`dfn-cert: DFN-CERT-2022-0026`
`dfn-cert: DFN-CERT-2021-2637`
`dfn-cert: DFN-CERT-2021-2560`
`dfn-cert: DFN-CERT-2021-2551`
`dfn-cert: DFN-CERT-2021-2544`
`dfn-cert: DFN-CERT-2021-2537`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2517`
`dfn-cert: DFN-CERT-2021-2513`
`dfn-cert: DFN-CERT-2021-2465`
`dfn-cert: DFN-CERT-2021-2422`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2280
dfn-cert: DFN-CERT-2021-2244
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2217
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2167
dfn-cert: DFN-CERT-2021-2157
dfn-cert: DFN-CERT-2021-2156
dfn-cert: DFN-CERT-2021-2154
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2145
dfn-cert: DFN-CERT-2021-2144
dfn-cert: DFN-CERT-2021-2143
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2092
dfn-cert: DFN-CERT-2021-2071
dfn-cert: DFN-CERT-2021-2030
dfn-cert: DFN-CERT-2021-2023
dfn-cert: DFN-CERT-2021-2022
dfn-cert: DFN-CERT-2021-2011
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1999
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1971
dfn-cert: DFN-CERT-2021-1955
dfn-cert: DFN-CERT-2021-1953
dfn-cert: DFN-CERT-2021-1949
dfn-cert: DFN-CERT-2021-1938
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1898
dfn-cert: DFN-CERT-2021-1897
dfn-cert: DFN-CERT-2021-1896
dfn-cert: DFN-CERT-2021-1895
dfn-cert: DFN-CERT-2021-1885
dfn-cert: DFN-CERT-2021-1879
dfn-cert: DFN-CERT-2021-1878
dfn-cert: DFN-CERT-2021-1852
dfn-cert: DFN-CERT-2021-1842
dfn-cert: DFN-CERT-2021-1836
dfn-cert: DFN-CERT-2021-1815
dfn-cert: DFN-CERT-2021-1783
dfn-cert: DFN-CERT-2021-1763

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1761
dfn-cert: DFN-CERT-2021-1754
dfn-cert: DFN-CERT-2021-1744
dfn-cert: DFN-CERT-2021-1707
dfn-cert: DFN-CERT-2021-1703
dfn-cert: DFN-CERT-2021-1699
dfn-cert: DFN-CERT-2021-1698
dfn-cert: DFN-CERT-2021-1697
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1621
dfn-cert: DFN-CERT-2021-1426

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:4777)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:4777 advisory.

Vulnerability Detection Result
Vulnerable package: kernel
Installed version: kernel-3.10.0-1160.el7
Fixed version: kernel-3.10.0-1160.49.1.el7

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: use-after-free in drivers/infiniband/core/ucma.c ctx use-after-free (CVE-2020-36385)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):
scsi: ibmvfc: Avoid link down on FS9100 canister reboot (BZ#1882627)
crash in qla2x00_status_entry() because of corrupt srb (BZ#1899599)
qedf driver: race condition between qedf's completion work task and another work item tearing down an fcport with qedf_cleanup_fcport (BZ#1941766)
The kernel crashes in hv_pci_remove_slots() upon hv device removal. A possible race between hv_pci_remove_slots() and pci_devices_present_work(). (BZ#1948961)
I/O delays incorrectly handled in the NVMe stack (BZ#1981610)
Data corruption in NFS client reusing slotid/seqid due to an interrupted slot (BZ#2007465)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:4777)`
OID:1.3.6.1.4.1.25623.1.0.883398
Version used: `2021-12-03T00:00:38Z`

References
`cve: CVE-2020-36385`
`advisory-id: CESA-2021:4777`
`url: https://lists.centos.org/pipermail/centos-announce/2021-December/048420.htm`
`↪l`
`cert-bund: CB-K21/0621`
`dfn-cert: DFN-CERT-2022-0103`
`dfn-cert: DFN-CERT-2021-2563`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2513`
`dfn-cert: DFN-CERT-2021-2497`
`dfn-cert: DFN-CERT-2021-2422`
`dfn-cert: DFN-CERT-2021-2386`
`dfn-cert: DFN-CERT-2021-2322`
`dfn-cert: DFN-CERT-2021-2321`
`dfn-cert: DFN-CERT-2021-2312`
`dfn-cert: DFN-CERT-2021-2280`
`dfn-cert: DFN-CERT-2021-2244`
`dfn-cert: DFN-CERT-2021-1696`
`dfn-cert: DFN-CERT-2021-1634`
`dfn-cert: DFN-CERT-2021-1617`
`dfn-cert: DFN-CERT-2021-1574`
`dfn-cert: DFN-CERT-2021-1546`
`dfn-cert: DFN-CERT-2021-1544`
`dfn-cert: DFN-CERT-2021-1480`
`dfn-cert: DFN-CERT-2021-1397`

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:0856)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:0856 advisory.

Vulnerability Detection Result

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.21.1.el7
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: Local buffer overflow in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c (CVE-2020-25211)
kernel: SCSI target (LIO) write to any block on ILO backstore (CVE-2020-28374)
kernel: locking issue in drivers/tty/tty_jobctrl.c can lead to an use-after-free (CVE-2020-29661)
kernel: malicious USB devices can lead to multiple out-of-bounds write (CVE-2019-19532)
kernel: out-of-bounds reads in pinctrl subsystem. (CVE-2020-0427)
kernel: use-after-free in i915_ppgtt_close in drivers/gpu/drm/i915/i915_gem_gtt.c (CVE-2020-7053)
kernel: performance counters race condition use-after-free (CVE-2020-14351)
kernel: Geneve/IPsec traffic may be unencrypted between two Geneve endpoints (CVE-2020-25645)
kernel: use-after-free in read in vt_do_kdgkb_ioctl (CVE-2020-25656)
kernel: ICMP rate limiting can be used for DNS poisoning attack (CVE-2020-25705)
kernel: increase slab leak leads to DoS (CVE-2021-20265)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):
BUG: scheduling while atomic: memory allocation under spinlock in scsi_register_device_handler() (BZ#1619147)
WARNING in __iscsit_free_cmd during recovery Abort (BZ#1784540)
lpfc does not issue adisc to fcp-2 devices, does not respond to nvme target that send an adisc. (BZ#1875961)
Panic in semctl_nolock.constprop.15+0x25b (BZ#1877264)RHEL 7.7> RHEL
[md]Crash due to invalid pool workqueue pointer, work queue race (BZ#1889372)
Guest crash on intel CPU with -cpu host, -spec-ctrl, +ibpb (BZ#1890669)
RHEL7.9 - kernel/uv: handle length extension properly (BZ#1899172)
Commit b144f013fc16a06d7a4b9a4be668a3583fafeda2 'i40e: don't report link up for a VF who hasn't enabled queues' introducing issues with VM using DPDK (BZ#1901064)
writing to /sys/devices/(...)/net/eno49/queues/tx-16/xps_cpus triggers kernel panic Hyper (BZ#1903819)Hyper-V>
[RHEL-7.9]video: hyperv_fb: Fix the cache type when mapping the VRAM Edit (BZ#1908896)
kvm-rhel7.9 [AMD] - system crash observed while powering on virtual machine with attached VF interfaces. (BZ#1909036)
kernel: nvme nvme7: Connect command failed, error wo/DNR bit: 2 (BZ#1910817)
dm-mirror crashes from assuming underlying storage will have a non-NULL merge_bvec_fn (BZ#1916407)
watchdog: use nmi registers snapshot in hardlockup handler (BZ#1916589)DELL EMC 7.9DELL EMC 7.9 BU BUG>
- Intel E810 NIC interfaces are not functional in RHEL 7.9 on system with AMD Rome CPUs DELL EMC BU (BZ#1918273)DELL EMC BUG>
RHEL system log shows AMD-Vi error when system connected with Gen 4 NVMe drives. (BZ#1921187)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:0856)`
OID:1.3.6.1.4.1.25623.1.0.883333
Version used: `2021-08-17T00:00:55Z`

References
`cve: CVE-2019-19532`
`cve: CVE-2020-0427`
`cve: CVE-2020-7053`
`cve: CVE-2020-14351`
`cve: CVE-2020-25211`
`cve: CVE-2020-25645`
`cve: CVE-2020-25656`
`cve: CVE-2020-25705`
`cve: CVE-2020-28374`
`cve: CVE-2020-29661`
`cve: CVE-2021-20265`
`advisory-id: CESA-2021:0856`
`url: https://lists.centos.org/pipermail/centos-announce/2021-March/048295.html`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K21/1268
cert-bund: CB-K21/0472
cert-bund: CB-K21/0283
cert-bund: CB-K21/0025
cert-bund: CB-K20/1225
cert-bund: CB-K20/1174
cert-bund: CB-K20/1163
cert-bund: CB-K20/1007
cert-bund: CB-K20/0998
cert-bund: CB-K20/0898
cert-bund: CB-K20/0873
cert-bund: CB-K20/0287
cert-bund: CB-K20/0162
cert-bund: CB-K20/0076
cert-bund: CB-K19/1079
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2399
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1563
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1292
dfn-cert: DFN-CERT-2021-1190
dfn-cert: DFN-CERT-2021-1178
dfn-cert: DFN-CERT-2021-1177
dfn-cert: DFN-CERT-2021-1139
dfn-cert: DFN-CERT-2021-1133
dfn-cert: DFN-CERT-2021-1013
dfn-cert: DFN-CERT-2021-0925
dfn-cert: DFN-CERT-2021-0888
dfn-cert: DFN-CERT-2021-0887
dfn-cert: DFN-CERT-2021-0825
dfn-cert: DFN-CERT-2021-0823
dfn-cert: DFN-CERT-2021-0765
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0699
dfn-cert: DFN-CERT-2021-0698
dfn-cert: DFN-CERT-2021-0697
dfn-cert: DFN-CERT-2021-0679
dfn-cert: DFN-CERT-2021-0676
dfn-cert: DFN-CERT-2021-0586
dfn-cert: DFN-CERT-2021-0579
dfn-cert: DFN-CERT-2021-0574

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0562
dfn-cert: DFN-CERT-2021-0561
dfn-cert: DFN-CERT-2021-0560
dfn-cert: DFN-CERT-2021-0509
dfn-cert: DFN-CERT-2021-0505
dfn-cert: DFN-CERT-2021-0497
dfn-cert: DFN-CERT-2021-0496
dfn-cert: DFN-CERT-2021-0468
dfn-cert: DFN-CERT-2021-0467
dfn-cert: DFN-CERT-2021-0426
dfn-cert: DFN-CERT-2021-0425
dfn-cert: DFN-CERT-2021-0424
dfn-cert: DFN-CERT-2021-0423
dfn-cert: DFN-CERT-2021-0422
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0356
dfn-cert: DFN-CERT-2021-0342
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2021-0327
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0313
dfn-cert: DFN-CERT-2021-0309
dfn-cert: DFN-CERT-2021-0298
dfn-cert: DFN-CERT-2021-0282
dfn-cert: DFN-CERT-2021-0280
dfn-cert: DFN-CERT-2021-0277
dfn-cert: DFN-CERT-2021-0264
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0261
dfn-cert: DFN-CERT-2021-0247
dfn-cert: DFN-CERT-2021-0221
dfn-cert: DFN-CERT-2021-0192
dfn-cert: DFN-CERT-2021-0191
dfn-cert: DFN-CERT-2021-0125
dfn-cert: DFN-CERT-2021-0116
dfn-cert: DFN-CERT-2021-0105
dfn-cert: DFN-CERT-2021-0100
dfn-cert: DFN-CERT-2021-0099
dfn-cert: DFN-CERT-2021-0084
dfn-cert: DFN-CERT-2021-0082
dfn-cert: DFN-CERT-2021-0081
dfn-cert: DFN-CERT-2021-0080
dfn-cert: DFN-CERT-2021-0079
dfn-cert: DFN-CERT-2021-0077
dfn-cert: DFN-CERT-2021-0076
dfn-cert: DFN-CERT-2021-0075

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0073
dfn-cert: DFN-CERT-2021-0041
dfn-cert: DFN-CERT-2021-0022
dfn-cert: DFN-CERT-2021-0021
dfn-cert: DFN-CERT-2021-0019
dfn-cert: DFN-CERT-2020-2772
dfn-cert: DFN-CERT-2020-2731
dfn-cert: DFN-CERT-2020-2730
dfn-cert: DFN-CERT-2020-2720
dfn-cert: DFN-CERT-2020-2715
dfn-cert: DFN-CERT-2020-2709
dfn-cert: DFN-CERT-2020-2705
dfn-cert: DFN-CERT-2020-2696
dfn-cert: DFN-CERT-2020-2686
dfn-cert: DFN-CERT-2020-2669
dfn-cert: DFN-CERT-2020-2665
dfn-cert: DFN-CERT-2020-2654
dfn-cert: DFN-CERT-2020-2612
dfn-cert: DFN-CERT-2020-2605
dfn-cert: DFN-CERT-2020-2602
dfn-cert: DFN-CERT-2020-2598
dfn-cert: DFN-CERT-2020-2597
dfn-cert: DFN-CERT-2020-2594
dfn-cert: DFN-CERT-2020-2592
dfn-cert: DFN-CERT-2020-2591
dfn-cert: DFN-CERT-2020-2580
dfn-cert: DFN-CERT-2020-2579
dfn-cert: DFN-CERT-2020-2562
dfn-cert: DFN-CERT-2020-2561
dfn-cert: DFN-CERT-2020-2555
dfn-cert: DFN-CERT-2020-2509
dfn-cert: DFN-CERT-2020-2493
dfn-cert: DFN-CERT-2020-2489
dfn-cert: DFN-CERT-2020-2488
dfn-cert: DFN-CERT-2020-2476
dfn-cert: DFN-CERT-2020-2450
dfn-cert: DFN-CERT-2020-2446
dfn-cert: DFN-CERT-2020-2376
dfn-cert: DFN-CERT-2020-2359
dfn-cert: DFN-CERT-2020-2291
dfn-cert: DFN-CERT-2020-2275
dfn-cert: DFN-CERT-2020-2274
dfn-cert: DFN-CERT-2020-2270
dfn-cert: DFN-CERT-2020-2243
dfn-cert: DFN-CERT-2020-2217
dfn-cert: DFN-CERT-2020-2156
dfn-cert: DFN-CERT-2020-1995

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-1969
dfn-cert: DFN-CERT-2020-1325
dfn-cert: DFN-CERT-2020-1319
dfn-cert: DFN-CERT-2020-1193
dfn-cert: DFN-CERT-2020-0999
dfn-cert: DFN-CERT-2020-0991
dfn-cert: DFN-CERT-2020-0974
dfn-cert: DFN-CERT-2020-0959
dfn-cert: DFN-CERT-2020-0929
dfn-cert: DFN-CERT-2020-0710
dfn-cert: DFN-CERT-2020-0543
dfn-cert: DFN-CERT-2020-0536
dfn-cert: DFN-CERT-2020-0478
dfn-cert: DFN-CERT-2020-0471
dfn-cert: DFN-CERT-2020-0467
dfn-cert: DFN-CERT-2020-0446
dfn-cert: DFN-CERT-2020-0445
dfn-cert: DFN-CERT-2020-0432
dfn-cert: DFN-CERT-2020-0430
dfn-cert: DFN-CERT-2020-0428
dfn-cert: DFN-CERT-2020-0427
dfn-cert: DFN-CERT-2020-0412
dfn-cert: DFN-CERT-2020-0375
dfn-cert: DFN-CERT-2020-0349
dfn-cert: DFN-CERT-2020-0347
dfn-cert: DFN-CERT-2020-0182
dfn-cert: DFN-CERT-2020-0125
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2020-0018
dfn-cert: DFN-CERT-2019-2704
dfn-cert: DFN-CERT-2019-2698
dfn-cert: DFN-CERT-2019-2693
dfn-cert: DFN-CERT-2019-2666
```

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:2314)

Summary

The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:2314 advisory.

Vulnerability Detection Result

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.31.1.el7
```

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: Integer overflow in Intel(R) Graphics Drivers (CVE-2020-12362)
kernel: Use after free via PI futex state (CVE-2021-3347)
kernel: use-after-free in n_tty_receive_buf_common function in drivers/tty/n_tty.c (CVE-2020-8648)
kernel: Improper input validation in some Intel(R) Graphics Drivers (CVE-2020-12363)
kernel: Null pointer dereference in some Intel(R) Graphics Drivers (CVE-2020-12364)
kernel: Speculation on pointer arithmetic against bpf_context pointer (CVE-2020-27170)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):
kernel crash when call the timer function (sctp_generate_proto_unreach_event) of sctp module (BZ#1707184)
SCSI error handling process on HP P440ar controller gets stuck indefinitely in device reset operation (BZ#1830268)
netfilter: reproducible deadlock on nft_log module autoload (BZ#1858329)
netfilter: NULL pointer dereference in nf_tables_set_lookup() (BZ#1873171)DELL EMC 7.9DELL EMC 7.9 Bu
Bug>
: No acpi_pad threads on top command for 'power cap policy equal to 0 watts' (BZ#1883174)
A race between i40e_ndo_set_vf_mac() and i40e_vsi_clear() in the i40e driver causes a use after free condition of the kmalloc-4096 slab cache. (BZ#1886003)
netxen driver performs poorly with RT kernel (BZ#1894274)
gendisk->disk_part_tbl->last_lookup retains pointer after partition deletion (BZ#1898596)
Kernel experiences panic in update_group_power() due to division error even with Bug 1701115 fix (BZ#1910763)
RHEL7.9 - zfcp: fix handling of FCP_RESID_OVER bit in fcp ingress path (BZ#1917839)
RHEL7.9 - mm/THP: do not access vma->vm_mm after calling handle_userfault (BZ#1917840)
raid: wrong raid io account (BZ#1927106)
qla2x00_status_cont_entry() missing upstream patch that prevents unnecessary ABRT/warnings (BZ#1933784)
RHEL 7.9.z - System hang caused by workqueue stall in qla2xxx driver (BZ#1937945)
selinux: setsebool can trigger a deadlock (BZ#1939091)Hyper-V> Hyper-
[RHEL-7] Cannot boot kernel 3.10.0-1160.21.1.el7.x86_64 on Hyper-V (BZ#1941841)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:2314)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.883351
Version used: 2021-08-17T00:00:01Z

References

cve: CVE-2020-8648
cve: CVE-2020-12362
cve: CVE-2020-12363
cve: CVE-2020-12364
cve: CVE-2020-27170
cve: CVE-2021-3347
advisory-id: CESA-2021:2314
url: https://lists.centos.org/pipermail/centos-announce/2021-June/048337.html
cert-bund: CB-K21/1268
cert-bund: CB-K21/0824
cert-bund: CB-K21/0725
cert-bund: CB-K21/0302
cert-bund: CB-K21/0145
cert-bund: CB-K21/0108
cert-bund: CB-K20/0517
cert-bund: CB-K20/0180
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1924
dfn-cert: DFN-CERT-2021-1846
dfn-cert: DFN-CERT-2021-1835
dfn-cert: DFN-CERT-2021-1833
dfn-cert: DFN-CERT-2021-1638
dfn-cert: DFN-CERT-2021-1565
dfn-cert: DFN-CERT-2021-1563
dfn-cert: DFN-CERT-2021-1562
dfn-cert: DFN-CERT-2021-1454
dfn-cert: DFN-CERT-2021-1359
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1250
dfn-cert: DFN-CERT-2021-1190
dfn-cert: DFN-CERT-2021-1178
dfn-cert: DFN-CERT-2021-1139
dfn-cert: DFN-CERT-2021-1133
dfn-cert: DFN-CERT-2021-1086
dfn-cert: DFN-CERT-2021-1084
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-0991
dfn-cert: DFN-CERT-2021-0824
dfn-cert: DFN-CERT-2021-0822
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0785
dfn-cert: DFN-CERT-2021-0784
dfn-cert: DFN-CERT-2021-0763

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0761
dfn-cert: DFN-CERT-2021-0759
dfn-cert: DFN-CERT-2021-0758
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0731
dfn-cert: DFN-CERT-2021-0698
dfn-cert: DFN-CERT-2021-0658
dfn-cert: DFN-CERT-2021-0655
dfn-cert: DFN-CERT-2021-0628
dfn-cert: DFN-CERT-2021-0614
dfn-cert: DFN-CERT-2021-0605
dfn-cert: DFN-CERT-2021-0590
dfn-cert: DFN-CERT-2021-0579
dfn-cert: DFN-CERT-2021-0548
dfn-cert: DFN-CERT-2021-0505
dfn-cert: DFN-CERT-2021-0491
dfn-cert: DFN-CERT-2021-0490
dfn-cert: DFN-CERT-2021-0486
dfn-cert: DFN-CERT-2021-0464
dfn-cert: DFN-CERT-2021-0398
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0342
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2021-0327
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0313
dfn-cert: DFN-CERT-2021-0298
dfn-cert: DFN-CERT-2021-0295
dfn-cert: DFN-CERT-2021-0282
dfn-cert: DFN-CERT-2021-0280
dfn-cert: DFN-CERT-2021-0264
dfn-cert: DFN-CERT-2021-0221
dfn-cert: DFN-CERT-2021-0215
dfn-cert: DFN-CERT-2020-2403
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-1710
dfn-cert: DFN-CERT-2020-1319
dfn-cert: DFN-CERT-2020-1257
dfn-cert: DFN-CERT-2020-1249
dfn-cert: DFN-CERT-2020-1248
dfn-cert: DFN-CERT-2020-1151
dfn-cert: DFN-CERT-2020-1041
dfn-cert: DFN-CERT-2020-0999
dfn-cert: DFN-CERT-2020-0991
dfn-cert: DFN-CERT-2020-0959
dfn-cert: DFN-CERT-2020-0933

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-0929
dfn-cert: DFN-CERT-2020-0875
dfn-cert: DFN-CERT-2020-0874
dfn-cert: DFN-CERT-2020-0872
dfn-cert: DFN-CERT-2020-0871
dfn-cert: DFN-CERT-2020-0663
dfn-cert: DFN-CERT-2020-0541
dfn-cert: DFN-CERT-2020-0536
dfn-cert: DFN-CERT-2020-0535
dfn-cert: DFN-CERT-2020-0521
dfn-cert: DFN-CERT-2020-0446
dfn-cert: DFN-CERT-2020-0445
dfn-cert: DFN-CERT-2020-0432
dfn-cert: DFN-CERT-2020-0428
dfn-cert: DFN-CERT-2020-0427
dfn-cert: DFN-CERT-2020-0412

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:2725)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:2725 advisory.

Vulnerability Detection Result
Vulnerable package: kernel
Installed version: kernel-3.10.0-1160.el7
Fixed version: kernel-3.10.0-1160.36.2.el7

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: size_t-to-int conversion vulnerability in the filesystem layer (CVE-2021-33909)
kernel: use-after-free in net/bluetooth/hci_event.c when destroying an hci_chan (CVE-2021-33034)
kernel: use-after-free in show_numa_stats function (CVE-2019-20934)
kernel: mishandles invalid descriptors in drivers/media/usb/gspca/xirlink_cit.c (CVE-2020-11668)
kernel: use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c (CVE-2021-33033)

... continues on next page ...

... continued from previous page ...

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):RHEL7.9.z> RHEL7.9.z
n_tty_open: 'BUG: unable to handle kernel paging request' (BZ#1872778)ESXi> ESXi
[RHEL7.8]'qp_alloc_hypercall result = -20' / 'Could not attach to queue pair with -20' with vSphere Fault Tolerance enabled (BZ#1892237)RHEL7.9> RHEL7.9
[s390x][Regression] Sino Nomine swapgen IBM z/VM emulated DASD with DIAG driver returns EOPNOTSUPP (BZ#1910395)
False-positive hard lockup detected while processing the thread state information (SysRq-T) (BZ#1912221)
RHEL7.9 zstream - s390x LPAR with NVMe SSD will panic when it has 32 or more IFL (pci) (BZ#1917943)
The NMI watchdog detected a hard lockup while printing RCU CPU stall warning messages to the serial console (BZ#1924688)
nvme hangs when trying to allocate reserved tag (BZ#1926825)REGRESSION> REGRESSION
'call into AER handling regardless of severity' triggers do_recovery() unnecessarily on correctable PCIe errors (BZ#1933663)
Module nvme_core: A double free of the kmalloc-512 cache between nvme_trans_log_temperature() and nvme_get_log_page(). (BZ#1946793)
sctp - SCTP_CMD_TIMER_START queues active timer kernel BUG at kernel/timer.c:1000! (BZ#1953052)Hyper-V> Hyper-V
[RHEL-7]When CONFIG_NET_POLL_CONTROLLER is set, mainline commit 2a7f8c3b1d3fee is needed (BZ#1953075)
Kernel panic at cgroup_is_descendant (BZ#1957719)Hyper-V> Hyper-V
[RHEL-7]Commits To Fix Kdump Failures (BZ#1957803)
IGMPv2 JOIN packets incorrectly routed to loopback (BZ#1958339)CKI kernel builds> CKI kernel builds
: x86 binaries in non-x86 kernel rpms breaks systemtap [7.9.z] (BZ#1960193)
mlx4: Fix memory allocation in mlx4_buddy_init needed (BZ#1962406)
incorrect assertion on pi_state->pi_mutex.wait_lock from pi_state_update_owner() (BZ#1965495)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:2725)`
OID:1.3.6.1.4.1.25623.1.0.883363
Version used: `2021-08-17T00:00:55Z`

References
`cve: CVE-2019-20934`
`cve: CVE-2020-11668`
`cve: CVE-2021-33033`
`cve: CVE-2021-33034`
`cve: CVE-2021-33909`
`advisory-id: CESA-2021:2725`
`url: https://lists.centos.org/pipermail/centos-announce/2021-July/048344.html`
`cert-bund: CB-K21/1268`
`cert-bund: CB-K21/1251`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K21/0775
cert-bund: CB-K21/0530
cert-bund: CB-K20/1219
cert-bund: CB-K20/0367
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2540
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2434
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2244
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1802
dfn-cert: DFN-CERT-2021-1744
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1722
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1692
dfn-cert: DFN-CERT-2021-1653
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1617
dfn-cert: DFN-CERT-2021-1608
dfn-cert: DFN-CERT-2021-1607
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1571
dfn-cert: DFN-CERT-2021-1565
dfn-cert: DFN-CERT-2021-1564
dfn-cert: DFN-CERT-2021-1563
dfn-cert: DFN-CERT-2021-1562
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1559
dfn-cert: DFN-CERT-2021-1558
dfn-cert: DFN-CERT-2021-1556
dfn-cert: DFN-CERT-2021-1555
dfn-cert: DFN-CERT-2021-1554
dfn-cert: DFN-CERT-2021-1553

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1552
dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1535
dfn-cert: DFN-CERT-2021-1531
dfn-cert: DFN-CERT-2021-1530
dfn-cert: DFN-CERT-2021-1515
dfn-cert: DFN-CERT-2021-1474
dfn-cert: DFN-CERT-2021-1436
dfn-cert: DFN-CERT-2021-1417
dfn-cert: DFN-CERT-2021-1416
dfn-cert: DFN-CERT-2021-1408
dfn-cert: DFN-CERT-2021-1406
dfn-cert: DFN-CERT-2021-1365
dfn-cert: DFN-CERT-2021-1364
dfn-cert: DFN-CERT-2021-1362
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1353
dfn-cert: DFN-CERT-2021-1339
dfn-cert: DFN-CERT-2021-1338
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1244
dfn-cert: DFN-CERT-2021-1243
dfn-cert: DFN-CERT-2021-1220
dfn-cert: DFN-CERT-2021-1218
dfn-cert: DFN-CERT-2021-1200
dfn-cert: DFN-CERT-2021-1048
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0342
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0116
dfn-cert: DFN-CERT-2021-0105
dfn-cert: DFN-CERT-2021-0100
dfn-cert: DFN-CERT-2021-0099
dfn-cert: DFN-CERT-2021-0084
dfn-cert: DFN-CERT-2021-0079
dfn-cert: DFN-CERT-2021-0076
dfn-cert: DFN-CERT-2021-0041
dfn-cert: DFN-CERT-2020-2721
dfn-cert: DFN-CERT-2020-2665
dfn-cert: DFN-CERT-2020-2448
dfn-cert: DFN-CERT-2020-2438
dfn-cert: DFN-CERT-2020-2403
dfn-cert: DFN-CERT-2020-1934

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-1257
dfn-cert: DFN-CERT-2020-1248
dfn-cert: DFN-CERT-2020-1244
dfn-cert: DFN-CERT-2020-1178
dfn-cert: DFN-CERT-2020-1085
dfn-cert: DFN-CERT-2020-1072
dfn-cert: DFN-CERT-2020-1064
dfn-cert: DFN-CERT-2020-1059
dfn-cert: DFN-CERT-2020-0875

High (CVSS: 7.8)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:1071)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:1071 advisory.

Vulnerability Detection Result
Vulnerable package: kernel
Installed version: kernel-3.10.0-1160.el7
Fixed version: kernel-3.10.0-1160.24.1.el7

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: out-of-bounds read in libiscsi module (CVE-2021-27364)
kernel: heap buffer overflow in the iSCSI subsystem (CVE-2021-27365)
kernel: iscsi: unrestricted access to sessions and handles (CVE-2021-27363)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):
Customer testing eMMC sees and intermittent boot problem on 7.8+, was not seen on 7.3 (BZ#1918916)
tcm loopback driver causes double-start of scsi command when work is delayed Azure (BZ#1925652)Azure>
[RHEL-7]Mellanox Patches To Prevent Kernel Hang In MLX4 (BZ#1925691)
A patch from upstream c365c292d059 causes us to end up leaving rt_nr_boosted in an incon-RHEL7.9.z sistent state, which causes a hard lockup. (BZ#1928082)RHEL7.9.z>
Add fix to update snd_wl1 in bulk receiver fast path (BZ#1929804)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:1071)`
OID:1.3.6.1.4.1.25623.1.0.883337
Version used: `2021-08-17T00:00:01Z`

References
`cve: CVE-2021-27363`
`cve: CVE-2021-27364`
`cve: CVE-2021-27365`
`advisory-id: CESA-2021:1071`
`url: https://lists.centos.org/pipermail/centos-announce/2021-April/048298.html`
`cert-bund: CB-K21/1268`
`cert-bund: CB-K21/0240`
`dfn-cert: DFN-CERT-2021-1634`
`dfn-cert: DFN-CERT-2021-1504`
`dfn-cert: DFN-CERT-2021-1295`
`dfn-cert: DFN-CERT-2021-1052`
`dfn-cert: DFN-CERT-2021-1026`
`dfn-cert: DFN-CERT-2021-1022`
`dfn-cert: DFN-CERT-2021-1013`
`dfn-cert: DFN-CERT-2021-0888`
`dfn-cert: DFN-CERT-2021-0887`
`dfn-cert: DFN-CERT-2021-0825`
`dfn-cert: DFN-CERT-2021-0824`
`dfn-cert: DFN-CERT-2021-0823`
`dfn-cert: DFN-CERT-2021-0822`
`dfn-cert: DFN-CERT-2021-0789`
`dfn-cert: DFN-CERT-2021-0785`
`dfn-cert: DFN-CERT-2021-0784`
`dfn-cert: DFN-CERT-2021-0759`
`dfn-cert: DFN-CERT-2021-0758`
`dfn-cert: DFN-CERT-2021-0740`
`dfn-cert: DFN-CERT-2021-0737`
`dfn-cert: DFN-CERT-2021-0731`
`dfn-cert: DFN-CERT-2021-0713`
`dfn-cert: DFN-CERT-2021-0699`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-0698
dfn-cert: DFN-CERT-2021-0697
dfn-cert: DFN-CERT-2021-0688
dfn-cert: DFN-CERT-2021-0679
dfn-cert: DFN-CERT-2021-0658
dfn-cert: DFN-CERT-2021-0655
dfn-cert: DFN-CERT-2021-0614
dfn-cert: DFN-CERT-2021-0564
dfn-cert: DFN-CERT-2021-0505
```

High (CVSS: 7.2)
NVT: CentOS: Security Advisory for bpftool (CESA-2020:5437)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2020:5437 advisory.

Vulnerability Detection Result

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.11.1.el7
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: metadata validator in XFS may cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt (CVE-2020-14385)
kernel: The flow_dissector feature allows device tracking (CVE-2019-18282)
kernel: Buffer over-read in crypto_authenc_extractkeys() when a payload longer than 4 bytes is not aligned. (CVE-2020-10769)
kernel: buffer uses out of index in ext3/4 filesystem (CVE-2020-14314)
kernel: umask not applied on filesystem without ACL support (CVE-2020-24394)
kernel: TOCTOU mismatch in the NFS client code (CVE-2020-25212)
kernel: improper input validation in ppp_cp_parse_cr function leads to memory corruption and read overflow (CVE-2020-25643)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

... continues on next page ...

... continued from previous page ...

Bug Fix(es):
WARNING in set_restore_sigmask at ./arch/x86/include/asm/thread_info.h:298 sigsus- i40e
pend+0x6d/0x70 (BZ#1704650)i40e>
VFs see other VF's outgoing traffic (BZ#1845677)Hyper-V> Hyper-V
[RHEL7] Two fixes for kdump over network (BZ#1846667)
Loop in __run_timers() because base->timer_jiffies is very far behind causes a lockup condition. (BZ#1849716)
XFS transaction overrun when running docker on VMWARE (overlay fs) (BZ#1857203)
RHEL 7.9 NVMe/IB - Host crash encountered during array upgrade (BZ#1857397)
False positive hard lockup detected while disabling the hard lockup detector via sysctl -w ker- Hyper-V
nel.watchdog=0 (BZ#1860661)Hyper-V>
[RHEL-7] Only notify Hyper-V for die events that are oops (BZ#1868130)
Linux kernel crash due to openvswitch module (BZ#1869190)
'nodfs' option not working when using SMB2+ (BZ#1873033)
RHEL7.7 zstream - ESS - kernel panic triggered by freelist pointer corruption (BZ#1873189)
destroy_cfs_bandwidth() is called by free_fair_sched_group() without calling init_cfs_bandwidth() (BZ#1878000)
NULL pointer at nvme_rdma_setup_ctrl+0x1c2/0x8d0 [nvme_rdma] when discover E5700 (BZ#1878950)
IB Infiniband RDMA mlx5_ib is freeing a kmalloc-512 cache that it does not own causing Azure
memory corruption. (BZ#1880184)Azure>
[RHEL7] Two Patches Needed To Enable Azure Host Time-syncing in VMs (BZ#1884735)
connect AF_UNSPEC on a connecting AF_INET6 socket returns an error (BZ#1886305)
Rebuilding the grub with the CPU flag 'avx' disabled (clearcpuid=156) triggers kernel panic in xor_avx_2() (BZ#1886792)
nf_conntrack_sctp.h is not usable due to a missing commit (BZ#1887975)
Starting pvmove on top of physical volumes on MD devices causes IO error on ongoing IO (BZ#1890059)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2020:5437)`
OID:1.3.6.1.4.1.25623.1.0.883313
Version used: `2021-07-06T00:00:40Z`

References
`cve: CVE-2019-18282`
`cve: CVE-2020-10769`
`cve: CVE-2020-14314`
`cve: CVE-2020-14385`
`cve: CVE-2020-24394`
`cve: CVE-2020-25212`
`cve: CVE-2020-25643`
`cesa: 2020:5437`
`url: https://lists.centos.org/pipermail/centos-announce/2020-December/048241.htm`
`↪l`
`cert-bund: CB-K20/1060`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K20/1030
cert-bund: CB-K20/0901
cert-bund: CB-K20/0898
cert-bund: CB-K20/0833
cert-bund: CB-K20/0671
cert-bund: CB-K20/0627
cert-bund: CB-K20/0162
cert-bund: CB-K20/0058
dfn-cert: DFN-CERT-2021-1084
dfn-cert: DFN-CERT-2021-0574
dfn-cert: DFN-CERT-2021-0426
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0359
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2020-2748
dfn-cert: DFN-CERT-2020-2705
dfn-cert: DFN-CERT-2020-2664
dfn-cert: DFN-CERT-2020-2612
dfn-cert: DFN-CERT-2020-2602
dfn-cert: DFN-CERT-2020-2594
dfn-cert: DFN-CERT-2020-2592
dfn-cert: DFN-CERT-2020-2580
dfn-cert: DFN-CERT-2020-2579
dfn-cert: DFN-CERT-2020-2522
dfn-cert: DFN-CERT-2020-2493
dfn-cert: DFN-CERT-2020-2476
dfn-cert: DFN-CERT-2020-2450
dfn-cert: DFN-CERT-2020-2448
dfn-cert: DFN-CERT-2020-2446
dfn-cert: DFN-CERT-2020-2438
dfn-cert: DFN-CERT-2020-2359
dfn-cert: DFN-CERT-2020-2325
dfn-cert: DFN-CERT-2020-2313
dfn-cert: DFN-CERT-2020-2283
dfn-cert: DFN-CERT-2020-2282
dfn-cert: DFN-CERT-2020-2275
dfn-cert: DFN-CERT-2020-2274
dfn-cert: DFN-CERT-2020-2270
dfn-cert: DFN-CERT-2020-2249
dfn-cert: DFN-CERT-2020-2243
dfn-cert: DFN-CERT-2020-2229
dfn-cert: DFN-CERT-2020-2228
dfn-cert: DFN-CERT-2020-2219
dfn-cert: DFN-CERT-2020-2217
dfn-cert: DFN-CERT-2020-2216
dfn-cert: DFN-CERT-2020-2186
dfn-cert: DFN-CERT-2020-2156

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-2102
dfn-cert: DFN-CERT-2020-2048
dfn-cert: DFN-CERT-2020-2046
dfn-cert: DFN-CERT-2020-2038
dfn-cert: DFN-CERT-2020-1998
dfn-cert: DFN-CERT-2020-1997
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1983
dfn-cert: DFN-CERT-2020-1982
dfn-cert: DFN-CERT-2020-1972
dfn-cert: DFN-CERT-2020-1971
dfn-cert: DFN-CERT-2020-1963
dfn-cert: DFN-CERT-2020-1946
dfn-cert: DFN-CERT-2020-1936
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1931
dfn-cert: DFN-CERT-2020-1929
dfn-cert: DFN-CERT-2020-1923
dfn-cert: DFN-CERT-2020-1922
dfn-cert: DFN-CERT-2020-1921
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1897
dfn-cert: DFN-CERT-2020-1895
dfn-cert: DFN-CERT-2020-1739
dfn-cert: DFN-CERT-2020-1736
dfn-cert: DFN-CERT-2020-1710
dfn-cert: DFN-CERT-2020-1709
dfn-cert: DFN-CERT-2020-1694
dfn-cert: DFN-CERT-2020-1693
dfn-cert: DFN-CERT-2020-1692
dfn-cert: DFN-CERT-2020-1449
dfn-cert: DFN-CERT-2020-1244
dfn-cert: DFN-CERT-2020-0430
dfn-cert: DFN-CERT-2020-0375
```

[return to 192.168.137.31]

2.1.2 Medium general/tcp

Medium (CVSS: 6.7)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:3327)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:3327 advisory.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`Vulnerable package: kernel`
`Installed version: kernel-3.10.0-1160.el7`
`Fixed version: kernel-3.10.0-1160.41.1.el7`

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: out-of-bounds write in xt_compat_target_from_user() in net/netfilter/x_tables.c (CVE-2021-22555)
kernel: race condition for removal of the HCI controller (CVE-2021-32399)
kernel: powerpc: RTAS calls can be used to compromise kernel integrity (CVE-2020-27777)
kernel: Local privilege escalation due to incorrect BPF JIT branch displacement computation (CVE-2021-29154)
kernel: lack a full memory barrier upon the assignment of a new table value in net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h may lead to DoS (CVE-2021-29650)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):
SAN Switch rebooted and caused (?) OpenStack compute node to reboot (BZ#1897576)
sysfs: cannot create duplicate filename '/class/mdio_bus/ixgbe-8100 (BZ#1915449)
XFS: read-only recovery does not update free space accounting in superblock (BZ#1921551)
The memcg_params field of kmem_cache struct contains an old slab address that is to small for the current size of memcg_limited_groups_array_size. (BZ#1951810)
Backport of upstream patch 'net: Update window_clamp if SOCK_RCVBUF is set ' into rhel-7 (BZ#1962196)
Kernel panic in init_cq_frag_buf (BZ#1962499)
futex: futex_requeue can potentially free the pi_state structure twice (BZ#1966856)
be_poll lockup doing ifenslave when netconsole using bond (BZ#1971744)
OCP4.7 nodes panic at BUG_ON in nf_nat_setup_info() (BZ#1972970)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:3327)`
OID:1.3.6.1.4.1.25623.1.0.883377
Version used: `2021-09-03T00:00:28Z`

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2020-27777
cve: CVE-2021-22555
cve: CVE-2021-29154
cve: CVE-2021-29650
cve: CVE-2021-32399
advisory-id: CESA-2021:3327
url: https://lists.centos.org/pipermail/centos-announce/2021-August/048356.html
cert-bund: CB-K21/1268
cert-bund: CB-K21/0727
cert-bund: CB-K21/0725
cert-bund: CB-K21/0502
cert-bund: CB-K21/0363
cert-bund: CB-K21/0329
cert-bund: CB-K20/1167
dfn-cert: DFN-CERT-2022-0103
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2157
dfn-cert: DFN-CERT-2021-2156
dfn-cert: DFN-CERT-2021-2071
dfn-cert: DFN-CERT-2021-1924
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1905
dfn-cert: DFN-CERT-2021-1852
dfn-cert: DFN-CERT-2021-1846
dfn-cert: DFN-CERT-2021-1845
dfn-cert: DFN-CERT-2021-1842
dfn-cert: DFN-CERT-2021-1837
dfn-cert: DFN-CERT-2021-1836
dfn-cert: DFN-CERT-2021-1835
dfn-cert: DFN-CERT-2021-1802
dfn-cert: DFN-CERT-2021-1783
dfn-cert: DFN-CERT-2021-1761
dfn-cert: DFN-CERT-2021-1742
dfn-cert: DFN-CERT-2021-1703
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1653
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1617
dfn-cert: DFN-CERT-2021-1608
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1571
dfn-cert: DFN-CERT-2021-1558
dfn-cert: DFN-CERT-2021-1556

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1555
dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1535
dfn-cert: DFN-CERT-2021-1515
dfn-cert: DFN-CERT-2021-1482
dfn-cert: DFN-CERT-2021-1474
dfn-cert: DFN-CERT-2021-1454
dfn-cert: DFN-CERT-2021-1417
dfn-cert: DFN-CERT-2021-1416
dfn-cert: DFN-CERT-2021-1365
dfn-cert: DFN-CERT-2021-1364
dfn-cert: DFN-CERT-2021-1362
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1353
dfn-cert: DFN-CERT-2021-1339
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1292
dfn-cert: DFN-CERT-2021-1244
dfn-cert: DFN-CERT-2021-1243
dfn-cert: DFN-CERT-2021-1222
dfn-cert: DFN-CERT-2021-1220
dfn-cert: DFN-CERT-2021-1140
dfn-cert: DFN-CERT-2021-1052
dfn-cert: DFN-CERT-2021-1028
dfn-cert: DFN-CERT-2021-1027
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-1022
dfn-cert: DFN-CERT-2021-1018
dfn-cert: DFN-CERT-2021-1017
dfn-cert: DFN-CERT-2021-1016
dfn-cert: DFN-CERT-2021-1015
dfn-cert: DFN-CERT-2021-0991
dfn-cert: DFN-CERT-2021-0986
dfn-cert: DFN-CERT-2021-0970
dfn-cert: DFN-CERT-2021-0799
dfn-cert: DFN-CERT-2021-0793
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0787
dfn-cert: DFN-CERT-2021-0785
dfn-cert: DFN-CERT-2021-0784
dfn-cert: DFN-CERT-2021-0765
dfn-cert: DFN-CERT-2021-0736
dfn-cert: DFN-CERT-2021-0665
dfn-cert: DFN-CERT-2021-0425
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0342

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0191
dfn-cert: DFN-CERT-2021-0116
dfn-cert: DFN-CERT-2021-0105
dfn-cert: DFN-CERT-2021-0100
dfn-cert: DFN-CERT-2021-0099
dfn-cert: DFN-CERT-2021-0084
dfn-cert: DFN-CERT-2021-0079
dfn-cert: DFN-CERT-2021-0077
dfn-cert: DFN-CERT-2021-0075
dfn-cert: DFN-CERT-2021-0022
dfn-cert: DFN-CERT-2021-0019
dfn-cert: DFN-CERT-2020-2721
dfn-cert: DFN-CERT-2020-2720
dfn-cert: DFN-CERT-2020-2709
dfn-cert: DFN-CERT-2020-2687
dfn-cert: DFN-CERT-2020-2686
dfn-cert: DFN-CERT-2020-2678
dfn-cert: DFN-CERT-2020-2677
dfn-cert: DFN-CERT-2020-2676
dfn-cert: DFN-CERT-2020-2659
dfn-cert: DFN-CERT-2020-2654
```

Medium (CVSS: 6.6)
NVT: CentOS: Security Advisory for bpftool (CESA-2020:5023)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2020:5023 advisory.

Vulnerability Detection Result

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.6.1.el7
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: buffer over write in vgacon_scroll (CVE-2020-14331)
kernel: net-sysfs: *_queue_add_kobject refcount issue (CVE-2019-20811)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):OSP13, mlx5> OSP13, mlx5
SRIOV VF still sending traffic when PF is down (BZ#1733181)
gpf panic in virtio_check_driver_offered_fxature+6 when running sg_inq on a dm map for a lost virtio_blk (BZ#1811893)
GPF panic in qlt_free_session_done+626 (BZ#1826127)Brazos > Brazos
'Core(s) per socket' and 'Socket' values are interchanged in lscpu output. (kernel) (BZ#1826306)
megaraid Aero: call trace observed during reboots (BZ#1828312)
Crash in mptscsih_io_done() due to buffer overrun in sense_buf_pool (BZ#1829803)
The qedf driver fails to re-establish the online F/C port state when the downstream F/C port is toggled unless a LIP is forced (BZ#1836443)
tcp_fragment() limit causes packet drop under normal TCP load (BZ#1847765)
ip link command shows state as UNKNOWN for MACVLAN interface (BZ#1848950)
Lenovo TS 7Z60 Cooper Lake: PCI BAR firmware bug (BZ#1849223)RHEL-7/mlx4> RHEL-7/mlx4
ipoib_flush ipoib_ib_dev_flush_light [ib_ipoib] (BZ#1858707)
Uprobes crashes processes under GDB - SIGTRAP and SIGSEGV (BZ#1861396)
kernel-3.10.0-1127.19.1.el7.x86_64 crashes after an SSH connection attempt when running as a Xen PV guest on AMD Epyc Rome (BZ#1882468)
Null ptr deref after nf_reinject->nf_queue_entry_release_refs hits Attempt to release error doing inet_sock_destruct() (BZ#1885682)
Users of kernel are advised to upgrade to these updated packages, which fix these bugs.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2020:5023)`
OID:1.3.6.1.4.1.25623.1.0.883300
Version used: `2021-07-06T00:00:40Z`

References
`cve: CVE-2019-20811`
`cve: CVE-2020-14331`
`cesa: 2020:5023`
`url: https://lists.centos.org/pipermail/centos-announce/2020-November/035868.htm`
`↪l`
`cert-bund: CB-K20/1030`
`cert-bund: CB-K20/0779`
`cert-bund: CB-K20/0523`
`dfn-cert: DFN-CERT-2021-0364`
`dfn-cert: DFN-CERT-2021-0262`
`dfn-cert: DFN-CERT-2020-2588`
`dfn-cert: DFN-CERT-2020-2490`
`dfn-cert: DFN-CERT-2020-2359`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-2283
dfn-cert: DFN-CERT-2020-2229
dfn-cert: DFN-CERT-2020-2215
dfn-cert: DFN-CERT-2020-2186
dfn-cert: DFN-CERT-2020-2102
dfn-cert: DFN-CERT-2020-2064
dfn-cert: DFN-CERT-2020-2048
dfn-cert: DFN-CERT-2020-1998
dfn-cert: DFN-CERT-2020-1997
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1983
dfn-cert: DFN-CERT-2020-1982
dfn-cert: DFN-CERT-2020-1981
dfn-cert: DFN-CERT-2020-1972
dfn-cert: DFN-CERT-2020-1971
dfn-cert: DFN-CERT-2020-1963
dfn-cert: DFN-CERT-2020-1936
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1934
dfn-cert: DFN-CERT-2020-1925
dfn-cert: DFN-CERT-2020-1922
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1834
dfn-cert: DFN-CERT-2020-1760
dfn-cert: DFN-CERT-2020-1736
dfn-cert: DFN-CERT-2020-1709
dfn-cert: DFN-CERT-2020-1684
dfn-cert: DFN-CERT-2020-1257
```

Medium (CVSS: 6.5)
NVT: Missing Linux Kernel mitigations for 'iTLB multihit' hardware vulnerabilities

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'iTLB multihit' hardware vulnerabilities.

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "itlb_mult
↪ihit" hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                  | Kernel status (SSH respo
↪nse)
```

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪----
/sys/devices/system/cpu/vulnerabilities/itlb_multihit | Processor vulnerable
Notes on the "Kernel status / SSH response" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the kernel doesn't know this
↪vulnerability yet and is not providing any mitigation which means the target s
↪ystem is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:
Solution type: VendorFix
Enable the mitigation(s) in the Linux Kernel or update to a more recent Linux Kernel.

Vulnerability Detection Method
Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'iTLB multihit' hardware vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108766
Version used: `2021-08-12T00:00:50Z`

Product Detection Result
Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2018-12207
url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/multihit.html
cert-bund: CB-K20/0691
cert-bund: CB-K19/0980
cert-bund: CB-K19/0978
dfn-cert: DFN-CERT-2020-1711
dfn-cert: DFN-CERT-2020-1538
dfn-cert: DFN-CERT-2020-1500
dfn-cert: DFN-CERT-2020-0333
dfn-cert: DFN-CERT-2020-0269
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2019-2644
dfn-cert: DFN-CERT-2019-2640
dfn-cert: DFN-CERT-2019-2568
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2461
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-2444
dfn-cert: DFN-CERT-2019-2421
dfn-cert: DFN-CERT-2019-2415
dfn-cert: DFN-CERT-2019-2407
dfn-cert: DFN-CERT-2019-2402
dfn-cert: DFN-CERT-2019-2399
dfn-cert: DFN-CERT-2019-2397
dfn-cert: DFN-CERT-2019-2392
dfn-cert: DFN-CERT-2019-2390
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2388
dfn-cert: DFN-CERT-2019-2387
dfn-cert: DFN-CERT-2019-2386
dfn-cert: DFN-CERT-2019-2385
dfn-cert: DFN-CERT-2019-2384
dfn-cert: DFN-CERT-2019-2381
dfn-cert: DFN-CERT-2019-2379
dfn-cert: DFN-CERT-2019-2378
dfn-cert: DFN-CERT-2019-2375
dfn-cert: DFN-CERT-2019-2372
dfn-cert: DFN-CERT-2019-2371
```

Medium (CVSS: 5.5)
NVT: CentOS: Security Advisory for kernel (CESA-2022:0063)

Summary
The remote host is missing an update for the 'kernel' package(s) announced via the CESA-2022:0063 advisory.

Vulnerability Detection Result

```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.53.1.el7
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'kernel' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.

... continues on next page ...

... continued from previous page ...

Security Fix(es):
kernel: perf_event_parse_addr_filter memory (CVE-2020-25704)
kernel: fuse: fuse_do_getattr() calls make_bad_inode() in inappropriate situations (CVE-2020-36322)
kernel: Heap buffer overflow in firedtv driver (CVE-2021-42739)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):
A gfs2 withdrawal occurs function = gfs2_setbit, file = fs/gfs2/rgrp.c, line = 109 (BZ#1364234)
i40e SR-IOV TX driver issue detected on VF 7 - VF connectivity loose after VF down/up (BZ#1977246)
duplicate ACK not sent when expected (BZ#1990665)kernel-debug> kernel-debug
BUG: bad unlock balance detected! when running LTP read_all (BZ#2006536)
Rudimentary support for AMD Milan - Call init_amd_zn() om Family 19h processors (BZ#2019218)
A VM with <=8 CPUs handles all the Mellanox NIC interrupts on CPU0 only, causing low performance (BZ#2019272)
fix _PSD override quirk for AMD family 19h+ (BZ#2019588)
generic_file_aio_read returns 0 when interrupted early with a fatal signal (BZ#2020857)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for kernel (CESA-2022:0063)`
OID:1.3.6.1.4.1.25623.1.0.884189
Version used: `2022-01-20T00:00:39Z`

References
`cve: CVE-2020-25704`
`cve: CVE-2020-36322`
`cve: CVE-2021-42739`
`advisory-id: CESA-2022:0063`
`url: https://lists.centos.org/pipermail/centos-announce/2022-January/073546.html`
`cert-bund: CB-K21/1086`
`cert-bund: CB-K21/0381`
`cert-bund: CB-K20/1114`
`dfn-cert: DFN-CERT-2022-0262`
`dfn-cert: DFN-CERT-2022-0261`
`dfn-cert: DFN-CERT-2022-0260`
`dfn-cert: DFN-CERT-2022-0258`
`dfn-cert: DFN-CERT-2022-0237`
`dfn-cert: DFN-CERT-2022-0194`
`dfn-cert: DFN-CERT-2022-0062`
`dfn-cert: DFN-CERT-2022-0058`
`dfn-cert: DFN-CERT-2022-0020`
`dfn-cert: DFN-CERT-2021-2637`
`dfn-cert: DFN-CERT-2021-2560`
`dfn-cert: DFN-CERT-2021-2544`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2343
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2321
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1416
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1222
dfn-cert: DFN-CERT-2021-1140
dfn-cert: DFN-CERT-2021-1084
dfn-cert: DFN-CERT-2021-1052
dfn-cert: DFN-CERT-2021-1027
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-1022
dfn-cert: DFN-CERT-2021-0799
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0426
dfn-cert: DFN-CERT-2021-0425
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0192
dfn-cert: DFN-CERT-2021-0022
dfn-cert: DFN-CERT-2020-2772
dfn-cert: DFN-CERT-2020-2731
dfn-cert: DFN-CERT-2020-2730
dfn-cert: DFN-CERT-2020-2709
dfn-cert: DFN-CERT-2020-2696
dfn-cert: DFN-CERT-2020-2686
dfn-cert: DFN-CERT-2020-2678
dfn-cert: DFN-CERT-2020-2676
dfn-cert: DFN-CERT-2020-2612
dfn-cert: DFN-CERT-2020-2605
dfn-cert: DFN-CERT-2020-2602
dfn-cert: DFN-CERT-2020-2598
dfn-cert: DFN-CERT-2020-2597
dfn-cert: DFN-CERT-2020-2591

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-2579
dfn-cert: DFN-CERT-2020-2496

Medium (CVSS: 5.5)
NVT: CentOS: Security Advisory for bpftool (CESA-2022:0063)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2022:0063 advisory.

Vulnerability Detection Result
Vulnerable package: kernel
Installed version: kernel-3.10.0-1160.el7
Fixed version: kernel-3.10.0-1160.53.1.el7

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: perf_event_parse_addr_filter memory (CVE-2020-25704)
kernel: fuse: fuse_do_getattr() calls make_bad_inode() in inappropriate situations (CVE-2020-36322)
kernel: Heap buffer overflow in firedtv driver (CVE-2021-42739)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):
A gfs2 withdrawal occurs function = gfs2_setbit, file = fs/gfs2/rgrp.c, line = 109 (BZ#1364234)
i40e SR-IOV TX driver issue detected on VF 7 - VF connectivity loose after VF down/up (BZ#1977246)
duplicate ACK not sent when expected (BZ#1990665)kernel-debug> kernel-debug
BUG: bad unlock balance detected! when running LTP read_all (BZ#2006536)
Rudimentary support for AMD Milan - Call init_amd_zn() om Family 19h processors (BZ#2019218)
A VM with <=8 CPUs handles all the Mellanox NIC interrupts on CPU0 only, causing low performance (BZ#2019272)
fix _PSD override quirk for AMD family 19h+ (BZ#2019588)
generic_file_aio_read returns 0 when interrupted early with a fatal signal (BZ#2020857)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: CentOS: Security Advisory for bpftool (CESA-2022:0063)
OID:1.3.6.1.4.1.25623.1.0.884190
Version used: 2022-01-20T00:00:39Z

References

cve: CVE-2020-25704
cve: CVE-2020-36322
cve: CVE-2021-42739
advisory-id: CESA-2022:0063
url: https://lists.centos.org/pipermail/centos-announce/2022-January/073549.html
cert-bund: CB-K21/1086
cert-bund: CB-K21/0381
cert-bund: CB-K20/1114
dfn-cert: DFN-CERT-2022-0262
dfn-cert: DFN-CERT-2022-0261
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0258
dfn-cert: DFN-CERT-2022-0237
dfn-cert: DFN-CERT-2022-0194
dfn-cert: DFN-CERT-2022-0062
dfn-cert: DFN-CERT-2022-0058
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2343
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2321
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1416
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1222
dfn-cert: DFN-CERT-2021-1140
dfn-cert: DFN-CERT-2021-1084

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-1052
dfn-cert: DFN-CERT-2021-1027
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-1022
dfn-cert: DFN-CERT-2021-0799
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0426
dfn-cert: DFN-CERT-2021-0425
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0192
dfn-cert: DFN-CERT-2021-0022
dfn-cert: DFN-CERT-2020-2772
dfn-cert: DFN-CERT-2020-2731
dfn-cert: DFN-CERT-2020-2730
dfn-cert: DFN-CERT-2020-2709
dfn-cert: DFN-CERT-2020-2696
dfn-cert: DFN-CERT-2020-2686
dfn-cert: DFN-CERT-2020-2678
dfn-cert: DFN-CERT-2020-2676
dfn-cert: DFN-CERT-2020-2612
dfn-cert: DFN-CERT-2020-2605
dfn-cert: DFN-CERT-2020-2602
dfn-cert: DFN-CERT-2020-2598
dfn-cert: DFN-CERT-2020-2597
dfn-cert: DFN-CERT-2020-2591
dfn-cert: DFN-CERT-2020-2579
dfn-cert: DFN-CERT-2020-2496
```

Medium (CVSS: 5.0)
NVT: CentOS: Security Advisory for bpftool (CESA-2021:3438)

Summary
The remote host is missing an update for the 'bpftool' package(s) announced via the CESA-2021:3438 advisory.

Vulnerability Detection Result
```
Vulnerable package: kernel
Installed version:  kernel-3.10.0-1160.el7
Fixed version:      kernel-3.10.0-1160.42.2.el7
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'bpftool' package(s) on CentOS 7.

Vulnerability Insight
The kernel packages contain the Linux kernel, the core of any Linux operating system.
Security Fix(es):
kernel: use-after-free in route4_change() in net/sched/cls_route.c (CVE-2021-3715)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Bug Fix(es):RHEL 7.8> RHEL 7.8
[s390x][DASD]Crash in __list_del_entry, alias_pav_group list corrupt when running dasd_alias_remove_device() (BZ#1889418)
EMBARGOED CVE-2021-3715 kernel: use-after-free in route4_change() in net/sched/cls_route.c (BZ#1992926)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `CentOS: Security Advisory for bpftool (CESA-2021:3438)`
OID:1.3.6.1.4.1.25623.1.0.883380
Version used: `2021-10-08T00:00:28Z`

References
`cve: CVE-2021-3715`
`advisory-id: CESA-2021:3438`
`url: https://lists.centos.org/pipermail/centos-announce/2021-September/048367.ht`
`↪ml`
`cert-bund: CB-K22/0130`
`cert-bund: CB-K21/0938`
`dfn-cert: DFN-CERT-2022-0224`
`dfn-cert: DFN-CERT-2022-0074`
`dfn-cert: DFN-CERT-2021-2560`
`dfn-cert: DFN-CERT-2021-2544`
`dfn-cert: DFN-CERT-2021-2537`
`dfn-cert: DFN-CERT-2021-2517`
`dfn-cert: DFN-CERT-2021-2441`
`dfn-cert: DFN-CERT-2021-2425`
`dfn-cert: DFN-CERT-2021-2414`
`dfn-cert: DFN-CERT-2021-2399`
`dfn-cert: DFN-CERT-2021-2342`
`dfn-cert: DFN-CERT-2021-2341`
`dfn-cert: DFN-CERT-2021-2315`
`dfn-cert: DFN-CERT-2021-2133`
`dfn-cert: DFN-CERT-2021-1993`
`dfn-cert: DFN-CERT-2021-1986`
`dfn-cert: DFN-CERT-2021-1905`
`dfn-cert: DFN-CERT-2021-1880`
`dfn-cert: DFN-CERT-2021-1879`
`dfn-cert: DFN-CERT-2021-1878`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1877

[return to 192.168.137.31]