There will be no additional articles for a little while.

There will be no new articles for a little while. This is not a bad thing! This is a good thing.

I have also stopped the automated security notices that get published. I will soon figure out a way to put the site into read-only mode.

Why?

Well, the .gq domain is a free domain. I paid for it, ’cause the registrar is fond of taking domain names that were free and got popular. So, it’s a paid domain name, but it’s in a ‘bad neighborhood’.

Truthfully, I knew this going in. I just didn’t care.

I’ve since decided that I want to be indexed and seen by the search engines. I’ve decided that I want to share with a larger audience. Initially, it was just a ‘meh’ project. Lately, I’ve been authoring new articles every two days and have been maintaining that schedule quite nicely.

That’s bigger/better/more than I expected. So, I’m going to go ahead and redo the site with the goal of making the site better and more accessible to everyone.

By the way, if you want to help, there will soon be plenty to do!

Anyhow, think of it like this: We’re moving to a new location!

(I’ve done very little, but I want to concentrate my efforts there rather than trying to keep up here.)

Where are we moving to? Why, none other than Linux Tips.

(That’s https://linux-tips.us.)

I figure it’ll take about a week to get the new domain up and running, but it may be sooner. I’ll be importing the content from here while still writing new articles. It’s gonna be fun! (And a butt-load of work.) I’ll take some of the good ideas from here, some new ideas for there, and make it even better.

So, that’s why there are no new articles – and why there will be no new articles at this domain. And now you know…

(Don’t bother signing up for the newsletter here. I’ll import the subscribers over there unless they don’t want to be. Let me know in the comments if you don’t want to be transferred to the new newsletter and I’ll just automatically transfer everyone else.)

[CentOS-announce] CESA-2021:0742 Important CentOS 7 screen Security Update

CentOS Errata and Security Advisory 2021:0742 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0742

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

30b844415ba647e65a9810574f3ded5e1fc1edd02e28f73cc44ee2c35e97baea screen-4.1.0-0.27.20120314git3c2946.el7_9.x86_64.rpm

Source:

8110b0f5f7bc0070b8cd656a7965d0f7d2f7c69102bbd80dbfc966ea718f96d8 screen-4.1.0-0.27.20120314git3c2946.el7_9.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce

USN-4911-1: Linux kernel (OEM) vulnerabilities

It was discovered that the Nouveau GPU driver in the Linux kernel did not
properly handle error conditions in some situations. A local attacker could

use this to cause a denial of service (system crash). (CVE-2020-25639)
Jan Beulich discovered that the Xen netback backend in the Linux kernel did
not properly handle certain error conditions under paravirtualization. An
attacker in a guest VM could possibly use this to cause a denial of service
(host domain crash). (CVE-2021-28038)

It was discovered that the fastrpc driver in the Linux kernel did not
prevent user space applications from sending kernel RPC messages. A local
attacker could possibly use this to gain elevated privileges. (CVE-2021-28375)

It was discovered that the fuse user space file system implementation in
the Linux kernel did not properly handle bad inodes in some situations. A
local attacker could possibly use this to cause a denial of service.
(CVE-2021-28950)

USN-4909-1: Linux kernel vulnerabilities

Loris Reiff discovered that the BPF implementation in the Linux kernel did
not properly validate attributes in the getsockopt BPF hook. A local
attacker could possibly use this to cause a denial of service

(system
crash). (CVE-2021-20194)
Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H. Schönherr
discovered that the Xen paravirtualization backend in the Linux kernel did
not properly propagate errors to frontend drivers in some situations. An
attacker in a guest VM could possibly use this to cause a denial of service
(host domain crash). (CVE-2021-26930)

Jan Beulich discovered that multiple Xen backends in the Linux kernel did
not properly handle certain error conditions under paravirtualization. An
attacker in a guest VM could possibly use this to cause a denial of service
(host domain crash). (CVE-2021-26931)

It was discovered that the network block device (nbd) driver in the Linux
kernel contained a use-after-free vulnerability during device setup. A
local attacker with access to the nbd device could use this to cause a
denial of service (system crash) or possibly execute arbitrary code.
(CVE-2021-3348)

USN-4912-1: Linux kernel

(OEM) vulnerabilities

Piotr Krysiuk discovered that the BPF JIT compiler for x86 in the Linux
kernel did not properly validate computation of branch displacements in
some situations. A local attacker could use this to cause a denial of
service (system crash) or possibly execute arbitrary code. (CVE-2021-29154)
It was discovered that a race condition existed in the binder IPC
implementation in the Linux kernel, leading to a use-after-free
vulnerability. A local attacker could use this to cause a denial of service
(system crash) or possibly execute arbitrary code. (CVE-2020-0423)

It was discovered that the HID multitouch implementation within the Linux
kernel did not properly validate input events in some situations. A
physically proximate attacker could use this to cause a denial of service
(system crash) or possibly execute arbitrary code. (CVE-2020-0465)

It was discovered that the eventpoll (aka epoll) implementation in the
Linux kernel contained a logic error that could lead to a use after free
vulnerability. A local attacker could use this to cause a denial of service
(system crash) or possibly execute arbitrary code. (CVE-2020-0466)

It was discovered that a race condition existed in the perf

subsystem of
the Linux kernel, leading to a use-after-free vulnerability. An attacker
with access to the perf subsystem could use this to cause a denial of
service (system crash) or possibly execute arbitrary code. (CVE-2020-14351)

It was discovered that the frame buffer implementation in the Linux kernel
did not properly handle some edge cases in software scrollback. A local
attacker could use this to cause a denial of service (system crash) or
possibly execute arbitrary code. (CVE-2020-14390)

It was discovered that a race condition existed in the hugetlb sysctl
implementation in the Linux kernel. A privileged attacker could use this to
cause a denial of service (system crash). (CVE-2020-25285)

It was discovered that the GENEVE tunnel implementation in the Linux kernel
when combined with IPSec did not properly select IP routes in some
situations. An attacker could use this to expose sensitive information
(unencrypted network traffic). (CVE-2020-25645)

Bodong Zhao discovered a use-after-free in the Sun keyboard driver
implementation in the Linux kernel. A local attacker could use this to
cause a denial of service or possibly execute arbitrary code. (CVE-2020-25669)

Shisong Qin and Bodong Zhao discovered that Speakup screen

reader driver in
the Linux kernel did not correctly handle setting line discipline in some
situations. A local attacker could use this to cause a denial of service
(system crash). (CVE-2020-27830)

It was discovered that the Marvell WiFi-Ex device driver in the Linux
kernel did not properly validate ad-hoc SSIDs. A local attacker could use
this to cause a denial of service (system crash) or possibly execute
arbitrary code. (CVE-2020-36158)

Loris Reiff discovered that the BPF implementation in the Linux kernel did
not properly validate attributes in the getsockopt BPF hook. A local
attacker could possibly use this to cause a denial of service (system
crash). (CVE-2021-20194)

Adam Zabrocki discovered that the kprobes subsystem in the Linux kernel did
not properly detect linker padding in some situations. A privileged
attacker could use this to cause a denial of service (system crash) or
possibly expose sensitive information. (CVE-2021-3411)

□□ discovered that the NFS implementation in the Linux kernel did not
properly prevent access outside of an NFS export that is a subdirectory of
a file system. An attacker could possibly use this to bypass NFS access
restrictions. (CVE-2021-3178)