[CentOS-announce] CESA-2021:0992 Important CentOS 7 firefox Security Update

CentOS Errata and Security Advisory 2021:0992 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0992

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

67cc5f25f8e6a42f9536eb9dbe7e22e3fab22c55d87d37db23cb90136913067e firefox-78.9.0-1.el7.centos.i686.rpm

44600066daf3f3b57b9e269737e0b0dfcd410f3a524fbbd74aec3162d6f84f7c firefox-78.9.0-1.el7.centos.x86_64.rpm

Source:

bedd47ac6fc527b008c2ed93845707f248f2a8eae9ad4201508728e2b54283ad firefox-78.9.0-1.el7.centos.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-4893-1: Firefox vulnerabilities

Multiple security issues were discovered in Firefox. If a user were
tricked into opening a specially crafted website, an attacker could
potentially exploit these to cause a denial of service, obtain sensitive
information, or execute arbitrary code. (CVE-2021-23981, CVE-2021-23982,
CVE-2021-23983, CVE-2021-23987, CVE-2021-23988)
It was discovered that extensions could open popup windows with control
of the window title in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to spook a website and trick the user into providing
credentials. (CVE-2021-23984)

It was discovered that the DevTools remote debugging feature

could be
enabled without an indication to the user. If a local attacker could
modify the browser configuration, a remote attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23985)

It was discovered that extensions could read the response of cross
origin requests in some circumstances. If a user were tricked into
installing a specially crafted extension, an attacker could potentially
exploit this to obtain sensitive information. (CVE-2021-23986)

How To: List PCI Information From The Terminal (lspci)

Continuing with a theme, this article will explain how to use the terminal to view what's attached via PCI (Peripheral Component Interconnect) to your computer. PCI devices are the ones in the add-on slots in your computer. They're typically internal devices, though you can get USB powered external devices with PCI-e slots, they kind of defeat the purpose. For this article, we'll be using lscpi.

You may also be interested in reading up about lshw and lscpu. I didn't intend for this to be a 'series' but that's what it's starting to look like. That's nice, however. They're small bites that let you sample the buffet that is the Linux terminal.

This one is just a little more complicated than the last. For

starters, you may not have lscpi immediately available. You may have it installed by default, but you might not. It really depends on your distro. Either way, it's in your default repositories.

If you don't have it installed, it's in the package 'pciutils'. So, use your package manager to install it. For example, with apt you'd do this:

[code]sudo apt install pciutils[/code]

Once you have it installed, you'll see the manual defines 'lspci' as:

> *lspci – list all PCI devices*

If you don't know, PCI devices are a class of devices that are add-ons to your motherboard. They're mostly the devices that go in the slots, such as graphics cards or sound cards. They can be used for all sorts of things, these days even being used for M.2 devices that hold SSD drives for rapid storage. They're great because they have a fast bus speed, meaning that your computer can interact with them faster because data moves faster in both directions than it does for, for example, a USB device.

Except PCI devices aren't just limited to the things that go in slots. Your motherboard probably uses that same spec to interact with other devices. For example, your Ethernet and sound card may be listed – even though they're 'on-board' and not actually add-on cards. That's your motherboard using the same sort of bus spec but not actually using a physical port. Additionally, there are different types of PCI specifications, but we don't need to get into that today.

And, well, once again the 'lspci' name tells you what it does, now that you know that's what it does. It lists PCI devices, just as the name implies. There are a couple of ways that

you'd realistically want to use it.

NOTE: The results from 'lspci' are drawn from the The PCI ID Repository and may actually not be accurate. Yup. You could get inaccurate results from this command, but we throw it around daily as though it's infallible. And now you know…

Where were we? Oh, yeah… We were going to use 'lscpi' for something useful. So, let's crack open that terminal by using your keyboard to press CTRL + ALT + T and we'll first enter:

[code]lspci[/code]

That will list all your PCI devices in a quick and easy to read list. You may also want to get the verbose output and that's done like:

[code]lspci -v[/code]

The output of that command should be fairly obvious. After all, it does what it says it does on the tin. That's also perhaps the more useful of the commands. It's definitely the one that I use most frequently.

If you take the numbers from the start of each line from the output of the above command and use the -t switch you'll actually get an understandable 'tree' output that will help you further understand what's going on inside your case without opening it up. If one PCI device has multiple entries (as many do) it'll make that easier to understand. It's simply:

[code]lspci -t[/code]

However you can easily put the two of those together and simply get a great verbose tree output with:

[code]lspci -vt[/code]

That's plenty easy to understand but some folks may find it a

bit overwhelming. I don't usually need that much information, so I tend to run the command without any switches. As I bounce between devices, it's enough to just check and make sure I know what I'm working with.

NOTE: Older versions required *-vvv* for verbose and *-tree* were needed to perform those operations. The current versions simply use the *-v* and *-t* switches.

And there you have it. Yet another way to view hardware information from within the terminal. You may have noticed a trend and probably can narrow down your guess as to what the next article is gonna be about! If lscpi's parent package is not installed, it's really easy to get and you can then run the command. If you don't have access to many tools, you almost certainly have access to this one.

Like always, thanks for reading. Be sure to sign up for the newsletter. I'll only send you site-related material and won't sell your email address to anyone. I promise, I won't ever send you any spam – just site stuff!

USN-3685-2: Ruby regression

USN-3685-1 fixed a vulnerability in Ruby. The fix for CVE-2017-0903 introduced
a regression in Ruby. This update fixes the problem.
Original advisory details:

Some of these CVE were already addressed in previous
USN: 3439-1, 3553-1, 3528-1. Here we address for
the remain releases.

It was discovered that Ruby incorrectly handled certain inputs.

An attacker could use this to cause a buffer overrun. (CVE-2017-0898)

It was discovered that Ruby incorrectly handled certain files. An attacker could use this to overwrite any file on the filesystem.
(CVE-2017-0901)

It was discovered that Ruby was vulnerable to a DNS hijacking vulnerability.
An attacker could use this to possibly force the RubyGems client to download
and install gems from a server that the attacker controls. (CVE-2017-0902)

It was discovered that Ruby incorrectly handled certain YAML files.
An attacker could use this to possibly execute arbitrary code. (CVE-2017-0903)

It was discovered that Ruby incorrectly handled certain files. An attacker could use this to expose sensitive information. (CVE-2017-14064)

It was discovered that Ruby incorrectly handled certain inputs.
An attacker could use this to execute arbitrary code. (CVE-2017-10784)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to inject a crafted key into a HTTP
response. (CVE-2017-17742)

It was discovered that Ruby incorrectly handled certain files. An attacker could possibly use this to execute arbitrary code. This update is only addressed to ruby2.0. (CVE-2018-1000074)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to cause a denial of service.
(CVE-2018-8777)

USN-4888-2: ldb vulnerabilities

USN-4888-1 fixed several vulnerabilities in ldb. This update provides
the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly
handled certain LDAP attributes. A remote attacker could possibly use this
issue to cause the LDAP server to crash, resulting in a denial of service.
(CVE-2021-20277)

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly
handled certain DN strings. A remote attacker could use this issue to
cause the LDAP server to crash, resulting in a denial of service, or
possibly execute arbitrary code. (CVE-2020-27840)