MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 34 No. 5, January 2022 Editor: Trevor Cordes

Next Meeting: January 11th, 2022 (Online Video Meeting)

Network Monitoring with Netdisco and LibreNMS

Netdisco is "a web-based network management tool suitable for small to very large networks." LibreNMS is "a fully featured network monitoring system that provides a wealth of features and device support." Which one is right for you? The answer to that depends on what you're looking to monitor. In this presentation, Gilbert Detillieux will describe and demo both of these web-based monitoring tools, and show some of the unique advantages of each one.

The latest meeting details are always at:
https://muug.ca/meetings/

Where to Find the Meeting:

This month we will continue to use the open source meeting software: Big Blue Button. If you haven't tried it yet, we recommend joining the meeting a little early to familiarize yourself with the controls.

The virtual meeting room will be open by 7:00 pm on January 11th, 2022 with the actual meeting starting at 7:30 pm. You do not need to install any special app or software to use Big Blue Button: you can use it via any modern web-cam-enabled browser by going to the website link above.

Please note that the meeting link will not be active until approx. 30 minutes before the actually meeting date and time.

Massive Exploit of the Month: Log4j

It's been a good while since a really big security vulnerability has rocked the IT world. This time it's Log4j's turn. Log4j, organized by the Apache Software Foundation, is used in many (most?) Java deployments for, uh, logging. It's especially prevalent in enterprise settings and even hardware (e.g. network) products. This bug is a rarity in that it garnered an actual *10.0 CRITICAL* score from NIST. So what is CVE-2021-44228?

Some genius a long while back decided that it was desirable for log messages or message parameters to be parsed for LDAP/JNDI addresses, and then fetch Java bytecode from those LDAP servers and run it. Because that makes perfect sense. Not.

I suppose this falls into the category of not sanitizing your output. For web programmers, this is the similar to a XSS attack, except one that can ruin your server, not just your users' browsing integrity. However, while programmers may be used to sanitizing output to send to HTML, most wouldn't think to sanitize output to their logging subsystem! In fact, sanitizing output to logs might defeat the purpose in that it may obfuscate errors and, therefore, retard debugging. So this is a solid fail on the part of Log4j programmers.

Checking the git history for the project, one can see they added many hundreds of lines of code to try to solve the bug. They quickly made the fix available for the world to pick up. Strangely, Linux distros took up to a few days to ship the fix. Luckily a workaround existed in simply disabling this JDNI/LDAP feature in a config file.

All was well with the world again... until a couple of days later when someone checked out their "fix" code and realized it was "incomplete in certain non-default configurations", or, in other words, Bad

Things could still happen. They initially thought these new Bad Things were limited to DoS attacks. But other people quickly realized malign "code execution" was still a thing and they upped this second CVE-2021-45046's score to 9.0 from 3.7.

This time the Log4j programmers said @*%$ it and just yanked all of this JNDI cruft out of the main product and are moving it to a module that no sane person will ever touch again. (Now, do Java... Kidding!)

Ralph Goers of the ASF said "dealing with [this bug] has shown the JNDI has significant security issues". Ya think?

https://uefi.io/second-log4j-vulnerability-cve-2021-45046-discovered-new-patch-released/

Solid Snake-Oil Disks

Tom's Hardware recently published an article about an SSD specifically designed for audiophiles. The manufacturer claims the drive gives audio "a special natural feeling, it becomes more smooth and calm, the thickness is slightly increased".

The article authors are (obviously) dubious, considering the fact that an SSD in no way can impact the subjective audio experience, assuming it is delivering the bits in time to the rest of the computer. If your cheap SSD is delivering the wrong 0's and 1's to your CPU and audio card, you have bigger problems than "powerless", "flattened" sound! (h/t Kevin)

https://www.tomshardware.com/amp/news/nvme-ssd-for-audiophiles

Dot Matrix Music

At a recent MUUG monthly video meeting Adam Thompson brought up a favourite esoteric audio CD release of ours: *Sypmhony #1 For Dot Matrix Printers*, by *[The User]*, released on obscure Dutch label *Staalplaat* in 1999. This is a release that should be owned by every self-styled nerd old enough to have lived through the dot matrix era.

The 16 "songs" are all brief, from 4 seconds to close to 3 minutes (on a 3" mini CD), all with wacky titles (only found in the data region of the CD) like *Login*, *New Existential Clause*, and *Random Telecom*.

Yes, all the songs are simply ASCII files played through numerous, old, synchronized dot matrix printers. Yes, they sound pretty much as you'd expect. However, some neat effects are achieved and you are encouraged to try to guess what characters are being printer in the quieter sections (I swear that's a comma...).

The album was met with so much critical acclaim that *[The User]* released a second symphony, with the incredibly different, imaginative and unexpected title of *Symphony #2 For Dot Matrix Printers*. This second release includes "remixes from Symphony #1 and new material". It also gets a domestic release on *Asphodel* in addition to *Staalplaat*. A sample track title is .^.^%^%^%, which I'm guessing is part of the sequence of characters being "played".

[The User] is, strangely enough, a duo from Montreal. They even have a third release, *Abandon*, which abandons the printers and dives into an old grain elevator in Montreal to produce strange sounds with crazy acoustics caused by the novel setting. One reviewer says it has "absolutely bowel quaking bass tones" providing "vacant fulfillment". Indeed!

https://www.discogs.com/artist/19885-The-User

http://www.undefine.ca/en/artists/the-user/

Intel Wants SDSi In Linux

Software Defined Silicon (SDSi) is gaining mainstream attention lately. It allows chip makers to turn on various advanced bells and whistles in hardware on demand; such as when you give them a lot of extra money. Big Iron has been doing this for a long time. The idea is you achieve economies of scale by shipping just one (or a few) products and then turning on/off features post-delivery. Imagine Intel having to make only one physical i7 CPU and then having each one morph into the desired SKU simply with a software-delivered code.

Recently, Intel submitted code into the Linux kernel to enable SDSi. Some people have been leery as the

code is fairly opaque and is not really testable because no applicable hardware yet exists. If such products are released in the future, expect hackers to go nuts cracking it so they can turn their $100 Celerons into $1000 i9s for free.

https://www.theregister.com/2021/12/13/chipzillas_mystery_linux_muckabout_is/

CentOS 8 EOL

Thanks Red Hat! Boy are we glad you took over CentOS! Yes, CentOS 8 has been relegated to End Of Life status as of December 31st, meaning you must migrate off it by yesterday; or preferably sooner. They only shortened its lifespan by, oh, seven years, as the originally announced EOL date was 2029.

Luckily Red Hat has told us it has come up with *CentOS Stream* to replace it, but strangely have also told us not to use it as an alternative to CentOS. So what do they want CentOS users to migrate to? *RHEL* of course! Thanks for playin', now start payin'.

It looks like new(ish)comer *Rocky Linux* might be winning the battle of the CentOS replacements. Rocky now provides a handy tool called *migrate2rocky* to convert your CentOS 8 installations into Rocky. Give it a try and let your fellow MUUGers know how it went! Backup first!

Of course, your editor still suggests Fedora is an even better replacement, as long as you can handle the rolling-esque 6-month upgrade cycle. If you stay 1 to 1.5 versions behind (i.e. the 6 months before the EOL) you should avoid most of the bleeding edge bugs. Contrary to popular belief, you can run and administer the latest Fedora just like it's CentOS 5; well, CentOS 5 with systemd and dnf. You are not forced to use Fedora Modular, NetworkManager, Wayland or any other of the newer "features": it all can be disabled and removed quite easily.

https://9to5linux.com/centos-linux-8-reached-end-of-life-its-time-to-migrate-to-an-alternative-os

MX Linux 21 Wins Fosspost 2021

News site fosspost.org has chosen MX Linux 21 as the "Best Linux Distro of 2021". Of course, that is a subjective choice, and fosspost appears to be coming at it from the perspective of novice and/or ex-Windows users.

> *Combining hardware support, low resources consumption and huge number of utility apps and deep functionality options... It all creates a wonderful Linux distribution for the average user. MX Linux 21 is one of the best Linux distributions out there to try, and we recommend any new user thinking of switching to Linux from Windows to test it out.*

MX combined antiX and MEPIS; in fact, the "M" in MX comes from MEPIS and the "X" from antiX. It is based on Debian 11. It's very capable on older hardware (from its antiX roots) and does not use systemd by default (though it is supported).

https://fosspost.org/mx-linux-21-review-best-distribution-2021/

Canada Feds Tracking Your Phone

Ontario's former privacy commissioner has sounded the alarm that PHAC, a Canadian federal government agency, has admitted using "cell-tower/operator location data" to track the location and movements of masses of Canadians throughout the pandemic.

Reading between the lines, it would appear they are using cell tower data (like tower triangulation) that would operate independently of GPS or "location services" on your phone. That would mean that all phones are vulnerable even if they have location services and/or GPS disabled. Neither would an app be required. It was done without any customer consent or notification, and with no option to opt out.

On December 16th, 2021, PHAC issued a Research for Proposal for a contractor to basically continue this tracking. PHAC claims the data is "de-identified" and does not "collect any individual mobility data".

PHAC released a statement saying:

In partnership with CRC, PHAC has been producing report summaries to look at how movement trends of the Canadian population have changed over the course of the pandemic, including identifying new patterns to help direct public health messaging, planning and policy development.

https://reclaimthenet.org/ontario-coronavirus-cellphone-tracking/

Cleaning Linux Kernel Dep Cruft

Ingo Molnar wants to do a comprehensive clean-up of the kernel's header dependencies and hierarchy with the hopes of speeding up kernel build time by 50-80%. Apparently after 30 years of open source development, C projects can get a lot of messy cross-dependency on header files. In many cases files will claim to depend on other files when they really don't.

There are about 10,000 main .h files in the kernel. Molnar is working on the mother of all patch sets that would make over 2200 commits, and alter over 50% of the entire 27.8 million line source tree.

A major part of his year-long work is his "fast-headers tree" which reduces the size of the default headers "by 1-2 orders of magnitude". Neither Kroah-Hartman, nor Linus have said "no" yet. Sounds like one of those projects that you think will take just a few days when you start, only to be sucked into a year of pain.

https://www.zdnet.com/article/cleaning-up-the-linux-kernels-dependency-hell-this-developer-is-proposing-2200-commit-changes/

Wozniak Wants "Right To Repair"

Apple co-founder Steve Wozniak has been putting his weight behind the "right to repair" movement. The idea is devices and products should be repairable instead of just throwaway-upon-first-problem like everything is these days. (This is slightly ironic because Apple is one of the worst offenders in this regard; however, Woz is hardly to blame for that.)

Companies inhibit [the right to repair] because it gives the companies power, control, over everything.

The EU is already at work on right to repair laws regarding laptops, phones, and more.

https://www.youtube.com/watch?v=CN1djPMooVY

Help us promote this month's meeting, by putting this poster up on your workplace bulletin board or other suitable public message board:

https://muug.ca/meetings/MUUGmeeting.pdf

A big thanks to Les.net for providing MUUG with free hosting and all that bandwidth! Les.net (1996) Inc. is a local provider of VoIP, Internet and Data Centre services. Contact **sales@les.net** by email, or +1 (204) 944-0009 by phone.

Thank You Michael W. Lucas

MUUG would like to thank Michael W. Lucas for donating one of his e-books every month as a door prize. You can view and purchase his tech books here:

https://www.tiltedwindmillpress.com/product-category/tech/

Creative Commons License