MUUGLines

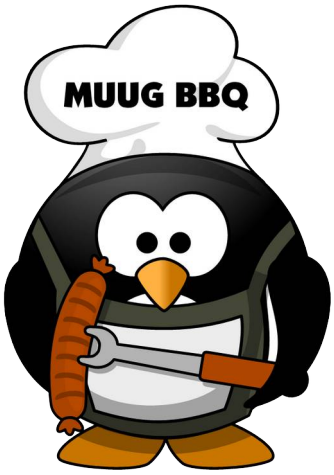
The Manitoba UNIX User Group Newsletter

Volume 36 No. 10-supplemental, July 2024 Editor: Trevor E Cordes

BBQ 2024 – All Invited!

Please RSVP Now!

BBQ Date: July 9th, 2024 – 6:30pm



It's summer again, and after a successful BBQ last year, we're doing it again. Everyone is welcome to attend: members and non-members alike. Come solo, or bring your family and kids. Help us make this event a success: we haven't had many RSVPs yet!

The location is the same as last year: Assiniboine Park, site #5, in the Northwest corner of the park.

Burgers and pop will be provided for free by MUUG. Feel free to bring your own food to share with others (potluck, chips, salad, whatever!) and your own beverages if you like. We will once again have a fire pit going, so you can even bring items that need to cook.

If it is raining to any large degree during the hours of the BBQ the date will be changed. All potential attendees are strongly encouraged to sign up to the MUUG-Announce e-mailing list to receive updated notices and information.

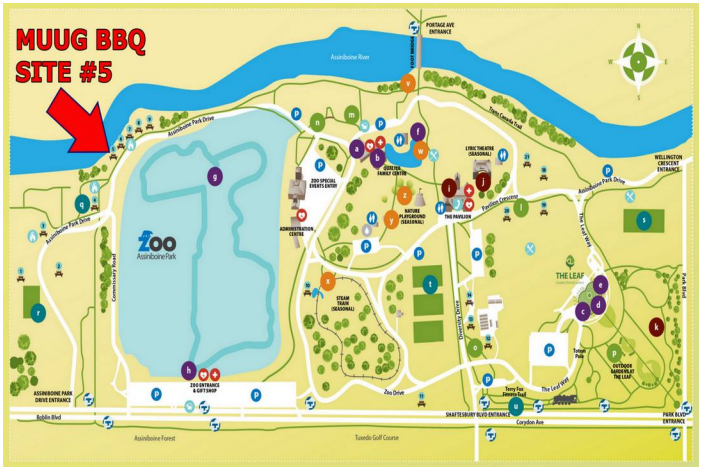
http://www.muug.ca/mailman/listinfo/muug-announce

RSVP via email to board@muug.ca with the subject "MUUG BBQ" before the extended deadline of July 7.

That will enable us to know how much food we need to buy. Make sure to tell us how many are coming!

Don't forget to bring your bug spray! Mosquitos in the west side of Winnipeg are brutal this year.

Regular meetings resume in the first week of September. This is your last chance to MUUG it up all summer!



Big Openssh Flaw

CVE-2024-6387 just hit the wires on July 2, and it's an "8.1 high" doozy. Normally most would shrug, but two days earlier a couple of important distros went EOL. Hmm, coincidence?

RHEL7, CentOS 7, and Debian 10 (and probably others) went EOL on June 30. Those still migrating those boxes (cough cough ehem) will have to take precautions.

The flaw is:

> *Possible remote code execution due to a race condition in signal handling*

Apparently pulling it off in the wild is quite difficult, and it the hacker isn't lucky or on point they are more likely to crash sshd than hack anything. However, that's not fun either.

Since the flaw requires no local access, no credentials, no user interaction, and can lead to remote code execution as root, it still qualifies as a "big one" in terms of "taking it seriously" levels.

The bug has to do with the LoginGraceTime default of 120 seconds, which uses SIGALRM under the hood. But some functions used in the interim, especially calls to syslog() are not async-signal-safe. This can cause heap corruption, which can, as usual, be exploited to run arbitrary code as openssh's user, which of course is root.

A mitigation exists where you simply set LoginGraceTime to 0 in sshd_config. That disables the grace timer completely and gives users unlimited time to login. However, this mitigation has a downside: hackers can now exhaust the limited number of simultaneous connections, thereby effecting a DoS. And to do so is trivial.

Another option is to use a firewall of some sort, like iptables, to limit what IP addresses can connect to ssh at all. Just make sure you don't accidentally lock yourself out of a remote box: if you only have dynamic IP addresses to play with, be extra careful. Or maybe implement some sort of port knocking.

Funny how this pops up 2 days after RHEL7 goes EOL, and not before. This author was just having discussions with a person in the process of migrating from 7 to 9, and it went something like "well, we get a grace period between June 30 and when the first nasty security hole appears, which is usually between a week to a couple of months". So much for that theory!

https://www.wiz.io/blog/cve-2024-6387-critical-rce-openssh

https://nvd.nist.gov/vuln/detail/CVE-2024-6387

When's That EOL Again?

While researching the above article, a great website was discovered that can help you track distros' (and other things') End Of Life(s).

https://endoflife.date/

Rather than hunting down each distro's date separately, you can just go there and get the info quickly and centrally. Now, to be really useful, it would be nice if that site let you see a calendar with each day showing the distros that went EOL on that day… In other words, to answer the question "how many and which distros went EOL on June 30" without having to click on 100 distros.

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

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

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