MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 38 No. 7, February 2026 Editor: Kevin Abedi

Next Meeting: February 3rd, 2026
In Person and Online

As usual, MUUG is meeting on the first Tuesday of the month. See below and to the right for location info.

Main Presentation – /bin Diving Duo

Wyatt Zacharias will dive into the /bin a couple times, and see what interesting nuggets can be found, studied, and explained this time. Wyatt may also do a more traditional RTFM-style presentation on a specific (and predetermined) command, such as *cowsay*. Come for the fun of it, stay for the group participation and shared learning opportunity!

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

If your MUUG membership has lapsed, please help support us by renewing today! Payment can be made via e-transfer, credit card, or PayPal here:
`https://muug.ca/about.php#payment`

Where to Find the Meeting:

NEW LOCATION

Winnipeg Senior Citizens Radio Club
598 St. Mary's Rd. Winnipeg, MB.

MUUG has moved to a new location to start the new season. Winnipeg Senior Citizens Radio Club (WSC) has graciously offered to host MUUG meetings going forward. Several current and past MUUG members are also members of WSC. MUUG President Wyatt Zacharias will be our WSC liaison and duty officer.

WSC is located at 598 St. Mary's Road, 2nd Floor, a block South from the St. Mary's / St. Anne's fork, on the West side beside the Miller's Meats. It's in the old fire hall, so you really can't miss it! Look for the red doors.

Please Remove Your Footwear

To keep the carpets clean and dry please remove your outdoor footwear at the top of the stairs.

Feel free to bring a pair of indoor shoes, sandals or Crocs to use indoors.

Entry Log Book

To support WSC operations, we ask all guests to sign the log book provided by WSC as you enter the meeting space.

The meeting space is on the **2nd floor** and there is no elevator, so attendees will have to be able to climb 1 flight of beautiful character style stairs. Apologies to anyone requiring accessibility. It is also possible to attend via online videoconferencing:
`https://muug.ca/meet`

GNU InetUtils Telnet Authentication Bypass – CVSS 9.8 / 10

A critical security vulnerability has been disclosed in the GNU *InetUtils telnet* daemon that has gone unnoticed for over a decade, leaving the root access open for attackers – of any system still running *telnet* that is.

The vulnerability, tracked as CVE-2026-24061, carries a CVSS severity score of 9.8 out of 10 and affects all GNU *InetUtils* releases from version from 1.9.3 to 2.7. According to the National Vulnerability Database (NVD), the vulnerability allows attackers to bypass remote authentication by using `-f root` value for the `USER` environment variable.

Simon Josefsson – A GNU contributor – explained on the *oss-security* mailing list that the issue is from how *telnetd* passes the `USER` variable provided by the client to the system's `/usr/bin/login` which typically runs as root. When using *telnet* login parameter and providing value of `-f root`, the client automatically is logged in as root and bypasses normal authentication. Essentially, its our "Little Bobby Tables" in action.

This new vulnerability is already attracting attention as GreyNoise intelligence indicates already attackers – originating from Hong Kong, the U.S., Japan, the Netherlands, China, Germany, Singapore, and Thailand – have been observed attempting to use the exploit.

Main recommendation from Josefsson is to not be running *telnet* at all, or at the very least, restrict network access for it to trusted client. Otherwise until a patch is available, *InetUtils telnet* can be configured to use a custom login(1) tool that does not allow the use of the `-f` parameter.

https://nvd.nist.gov/vuln/detail/CVE-2026-24061

https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html

https://seclists.org/oss-sec/2026/q1/89

FSF Effort on Keeping Their Software Free – BigBlueButton and MongoDB

Ian Kelling, senior systems administrator and president of the Free Software Foundation (FSF), has published a report detailing some of behind the scenes work of FSF that ensures the organization's technical infrastructure relies exclusively on free software.

FSF's tech team, consisting of only two people, is responsible for maintaining services, platforms and websites for FSF staff, GNU projects, other community projects, and the wider free software community.

While the tech team is mostly largely out of public view, their work is essential to everyday operations such as hosting conferences, scheduling meetings, and processing financial transactions.

Kelling explains how finding appropriate software among hundreds of thousands is a continues challenge, and how it involves checking the availability of source code, and the licences of the software and its dependencies. And to share their results, FSF runs the Free Software Directory that is a collection of verified free software.

FREE SOFTWARE FOUNDATION

A recent example of their efforts involves the videoconferencing platform BigBlueButton (BBB). BBB inadvertently picked up MongoDB's 2018 nonfree license change when its went from GNU Affero General Public License (AGPL) to the Server Side Public License (SSPL). FSF in collaboration with the developers and the community contributed to architectural changes that ultimately enabled BBB to removed MongoDB as a dependency. With the release of BigBlueButton 3.0 in 2025, it is now back to being a fully free software!

Kelling also adds how confusion and misinterpretation around licensing is not a new or an uncommon issue. While FSF has a licensing team which reviews licenses and publishes their findings, they are not able to publish an evaluation of each free license out there.

If you wish to help FSF, you can always get a membership at FSF to support their work and keep the momentum in the free software movement.

https://www.fsf.org/blogs/community/2026-values-into-practice

Geomagnetic Storm – January 19th-21th

On January 19th, National Oceanic and Atmospheric Administration (NOAA) issued a G4 (Severe) geomagnetic storm watch for expecting the arrival of coronal mass ejection (CME), launched from the

Sun on January 18th. While the storm watch was issued for January 20th, NOAA advised that levels G1-G3 could be reached by late Jan 19.

Despite the predictions, G4 levels were reached immediately as CME arrived, a mere 5 hours after the warning was issued.

Geomagnetic storms happen when disturbances from the Sun interact with Earth's magnetic field, potentially affecting modern technology. CMEs can cause geomagnetic storms at Earth degrading signal from radio navigation, disrupt satellite operation, and in extreme cases induce extra currents in the ground that can affects power grids.

In February 2022, SpaceX lost 38 Starlink satellites after a geomagnetic storm increased atmospheric density, causing the newly launched satellites to experience higher drag and reenter Earth's atmosphere prematurely.

Taken by Alexandre Croisier on January 19, 2026 @ Lighthouse of Pontusval, Brittany, France

On a positive note, the storm resulted in some beautiful sightings of Aurora across Europe and the US.

`https://www.swpc.noaa.gov/news/g4-severe-geomagnetic-storm-watch-20-january-utc-day`

`https://www.swpc.noaa.gov/news/g4-severe-geomagnetic-storm-levels-reached-19-jan-2026`

`https://spaceweather.com/archive.php?view=1&day=20&month=01&year=2026`

`https://www.spacex.com/updates#sustainability`

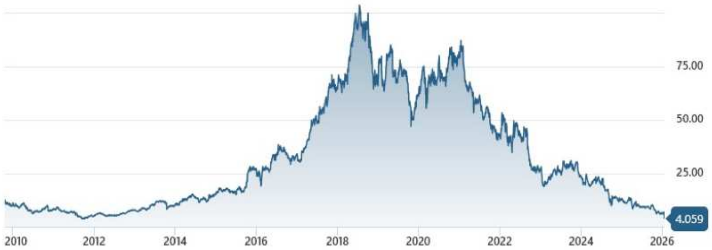
Ubisoft Shares Fall 33% After Announcement of Major Corporate Restructuring

Ubisoft's share price fell sharply on Thursday January 22nd, following the company's announcement of a wide-ranging internal restructuring planning for a "major company reset." UBISOFT

The plan involves splitting the creative operations into five separate divisions, a process that has reportedly been in development for approximately a year. Ubisoft claims that the changes are intended to help the company "reclaim its creative leadership" and "drive a sharp rebound" after its lackluster performance for several years.

Ubisoft is also abandoning development of six titles, delaying seven more, while also closing studios in Halifax and Stockholm with restructurings expected to happen in other countries.

Despite the goals and fancy corporate language, the market was not pleased. Ubisoft's share price dropped by over 30% in morning trading next day. At the time of writing, shares are trading at €4.06, down from €6.64 at Wednesday's market close.



The rise and fall of Ubisoft's stock prices since 2010. Last time prices where this low was late 2011.

`https://www.videogameschronicle.com/news/ubisoft-shares-drop-33-following-its-major-company-reset-announcement/`

`https://www.msn.com/en-us/money/markets/ubisoft-shares-tumble-after-assassin-s-creed-creator-unveils-restructuring-cancels-games/ar-AA1UJbTx`

Cloudflare WAF Bypass Vulnerability has been fixed

A critical vulnerability in Cloudflare's Web Application Firewall (WAF) had been allowing attackers to bypass protections and reach origin servers directly. The issue, discovered by the security research group *FearsOff*, was based on `/.well-known/acme-challenge/` directory, a path used for automated SSL/TLS certificate validation.

The vulnerability stemmed from Cloudflare's handling of the Automatic Certificate Management Environment (ACME) protocol, which is widely used by Certificate Authorities to verify domain ownership. To make the process easier, Cloudflare had disabled certain WAF checks on the ACME challenge path so that validation tokens could be served without interference.

However, FearsOff found that the ACME challenge path bypassed normal WAF and customer configuration ending up at the host server, even if everything was set to be blocked.

The researchers reported the issue to Cloudflare on October 9 through the company's HackerOne bug bounty program and a permanent fix was deployed on October 27.

Cloudflare noted that customers do not need to take any action and reported no evidence that the vulnerability was exploited in real-world attacks prior to the fix.

https://fearsoff.org/research/cloudflare-acme

https://blog.cloudflare.com/acme-path-vulnerability/

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

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

Our Corporate Sponsors:

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.

Thanks to Linux Mag for providing MUUG a half price magazine subscription for our door prizes.

Linux Magazine is your guide to the world of Linux and open source. Each monthly issue includes advanced technical information you won't find anywhere else including tutorials, in-depth articles on trending topics, troubleshooting and optimization tips, and more! Subscribe to their free newsletters and get news and articles in your inbox.

https://www.linux-magazine.com/