Published on *Tux Machines* (http://www.tuxmachines.org)

Security Leftovers

By *Roy Schestowitz*
Created *22/05/2019 - 10:06am*
Submitted by Roy Schestowitz on Wednesday 22nd of May 2019 10:06:37 AM Filed under Security [1]

- **WannaCry? Hundreds of US schools still haven?t patched servers [2]**

  > But cities aren't the only highly vulnerable targets to be found by would-be attackers. There are hundreds of thousands of Internet-connected Windows systems in the United States that still appear to be vulnerable to an exploit of Microsoft Windows' Server Message Block version 1 (SMB v. 1) file sharing protocol, despite repeated public warnings to patch systems following the worldwide outbreak of the WannaCry cryptographic malware two years ago. And based on data from the Shodan search engine and other public sources, hundreds of them?if not thousands?are servers in use at US public school systems.

- **Google stored some passwords in plain text for fourteen years [3]**

  > In a blog post today, Google disclosed that it recently discovered a bug that caused some portion of G Suite users to have their passwords stored in plain text. The bug has been around since 2005, though Google says that it can?t find any evidence that anybody?s password was improperly accessed. It?s resetting any passwords that might be affected and letting G Suite administrators know about the issue.
  >
  > G Suite is the corporate version of Gmail and Google?s other apps, and apparently the bug came about in this product because of a feature designed specifically for companies. Early on, it was possible for your company administrator for G Suite apps to set user passwords manually ? say, before a new employee came on board ? and if they did, the admin console would store those passwords in plain text instead of hashing them. Google has since removed that capability from administrators.

-

Notifying administrators about unhashed password storage
[4]

- **Google Disappoints Yet Again: Stored Some Passwords In Plain Text For 14 Years [5]**

  > G Suite users were taken aback yesterday when Google disclosed that it stored some passwords for Enterprise G Suite users in plain text for 14 years.
  >
  > In a blog post, the search giant mentioned that the passwords were encrypted but not hashed, which means that Google employees had complete access to them. However, the company says that there is no evidence that passwords were illegally accessed by anyone or misused.

- **Stable Version Of Tor Browser For Android Now Available On Play Store [6]**

  > After eight months of testing, a stable release for the Tor browser has arrived on the Play Store. The new Android browser now brings Tor features directly into a standalone browser, replacing the Orbot/Orfox as the main way to connect to the Tor network via Android devices.
  >
  > The stable version (v8.5) of Tor for Android routes your web traffic through the Tor network ? a web of encrypted computers spread worldwide.

Security

Source URL: http://www.tuxmachines.org/node/124133

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://arstechnica.com/information-technology/2019/05/two-years-after-wannacry-us-schools-still-vulnerable-to-eternalblue/
[3] https://www.theverge.com/2019/5/21/18634842/google-passwords-plain-text-g-suite-fourteen-years
[4] https://cloud.google.com/blog/products/g-suite/notifying-administrators-about-unhashed-password-storage
[5] https://fossbytes.com/google-stored-passwords-plain-text-for-14-years/
[6] https://fossbytes.com/stable-version-of-tor-browser-for-android-now-available-on-play-store/