Security and Fear, Uncertainty, Doubt (FUD) Tactics

By Roy Schestowitz
Created 10/03/2021 - 10:28pm
Submitted by Roy Schestowitz on Wednesday 10th of March 2021 10:28:41 PM Filed under Security [1]

- Security updates for Wednesday [2]
  Security updates have been issued by Debian (kernel and privoxy), Fedora (libtpms, privoxy, and x11vnc), openSUSE (chromium), Red Hat (.NET 5.0, .NET Core, .NET Core 2.1, .NET Core 3.1, dotnet, and dotnet3.1), SUSE (git, kernel, openssl-1_1, and wpa_supplicant), and Ubuntu (git and openssl).

- [Older] Use JoomScan to scan Joomla for vulnerabilities on Kali [3]
  When installing a content management system for your website, it's easy to get lazy and assume that it's going to do all the work for you. A CMS like Joomla certainly does make things more convenient, and lets you publish a polished website very quickly, but that doesn't mean you shouldn't take some extra time to secure it.

- Microsoft Security Researcher Proposes Unprivileged Chroot For Linux [4] [Ed: The same company that puts back doors in everything for the NSA is now posing as "security"; watch the replies in comments [5]]
  Security researcher and Microsoft engineer Mickaël Salaün is proposing unprivileged chroot support for the Linux kernel.

- Scanning for Secrets in Source Code [6] [Ed: Wrongly insinuating people all use Microsoft proprietary software (NSA PRISM) prison called GitHub]
As a developer, I admit that I’ve committed secrets to public Github repositories before. Hardcoded secrets have always been a problem in organizations and are one of the first things I look for during a penetration test. When developers write secrets such as passwords and API keys directly into source code, these secrets can make their way to public repos or application packages, then into an attacker’s hands. As microservice architectures and API-centric applications become mainstream, developers often need to exchange credentials and other secrets programmatically. This means that developers can sometimes make mistakes when handling sensitive data.

- Researchers Unveil New Linux Malware Linked to Chinese Hackers [7] [Ed: It seems possible that right about now, in order to distract from the Microsoft Exchange catastrophe (Microsoft uses xenophobia for blame-passing [8]), they will spam or Googlebomb "Linux" with China malware something]

  Cybersecurity researchers on Wednesday shed light on a new sophisticated backdoor targeting Linux endpoints and servers that's believed to be the work of Chinese nation-state actors.

Security

Source URL: http://www.tuxmachines.org/node/148671

Links:
[2] https://lwn.net/Articles/848973/rss