Security Leftovers

By Roy Schestowitz
Created 28/11/2021 - 1:19pm
Submitted by Roy Schestowitz on Sunday 28th of November 2021 01:19:46 PM

- New Side-Channel Vulnerability in the Linux Kernel Enabling DNS Cache Poisoning [1]
  
  A recent research paper by a team at University of California, Riverside, shows the existence of previously overlooked side channels in the Linux kernels that can be exploited to attack DNS servers.

  According to the researchers, the issue with DNS roots in its design, that never really took security as a key concern and that made it extremely hard to retrofit strong security features into it.

- Reproducible Builds (diffoscope): diffoscope 194 released [2]
  
  The diffoscope maintainers are pleased to announce the release of diffoscope version 194. This version includes the following changes:

  [ Chris Lamb ]
  * Don't traceback when comparing nested directories with non-directories
  (Closes: reproducible-builds/diffoscope#288)

- Thousands of printers at risk of denial of service attacks [3]
  
  Researchers have highlighted a trio of potential attacks against printers that could allow denial of service, information theft, or botnet compromise.

  The collection of attacks, labeled Printjack, appeared in a paper from researchers Giampaolo Bella and Pietro Biondi at the Università di Catania and Istituto di Informatica e Telematica in Italy.
GoDaddy says information on 1.2 million customers exposed in data breach[4]

In a document filed to the Securities and Exchange Commission on Monday, GoDaddy noted that the company had discovered its Managed WordPress hosting environment had been compromised by an ?unauthorized third party,? resulting in emails and customers numbers of 1.2 million Managed WordPress users being exposed.

Source URL: http://www.tuxmachines.org/node/158468

Links: