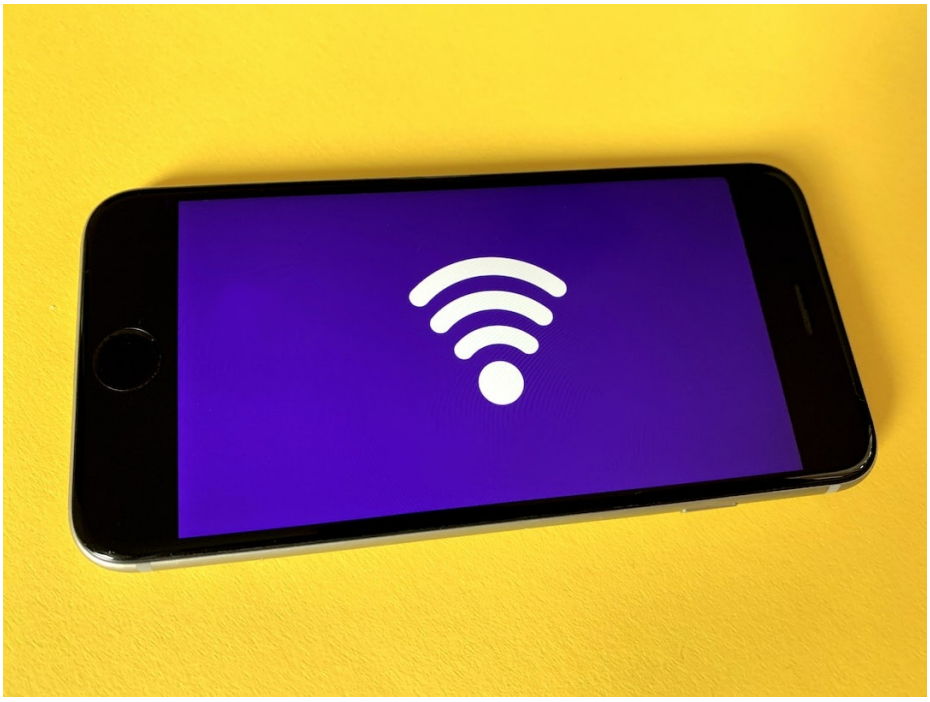
CyberSec Weekly

Happy Monday!

Welcome to the 34th Issue of CyberSec Weekly.

In this issue:



New Wi-Fi Protocol Security Flaw Affecting Linux, Android and iOS Devices

A group of academics from Northeastern University and KU Leuven has disclosed a fundamental design flaw in the IEEE 802.11 Wi-Fi protocol standard, impacting a wide range of devices running Linux, FreeBSD, Android, and iOS.

Successful exploitation of the shortcoming could be abused to hijack TCP connections or intercept client and web traffic, researchers Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef said in a paper

published this week.

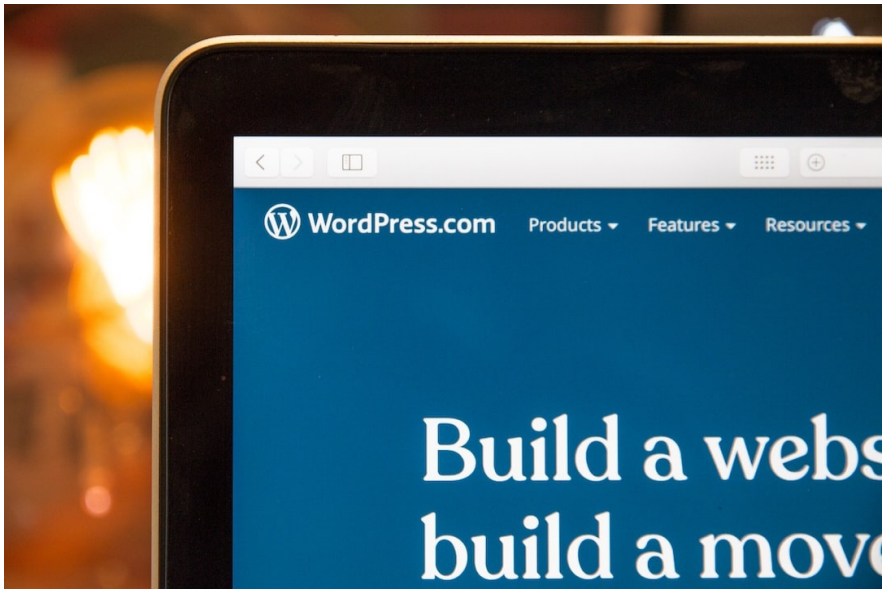
The approach exploits power-save mechanisms in endpoint devices to trick access points into leaking data frames in plaintext, or encrypt them using an all-zero key.

To read the full story...

Click Here

What's a sheep's favourite part of the computer?

The RAM.



Hackers Exploiting WordPress Elementor Pro Vulnerability

Unknown threat actors are actively exploiting a recently patched security vulnerability in the Elementor Pro website builder plugin for WordPress. The flaw, described as a case of broken access control, impacts versions 3.11.6 and earlier. It was addressed by the plugin maintainers in version 3.11.7 released on March 22.

"Improved code security enforcement in WooCommerce components," the Tel Aviv-based company said in its release notes. The premium plugin is estimated to be used on over 12 million sites.

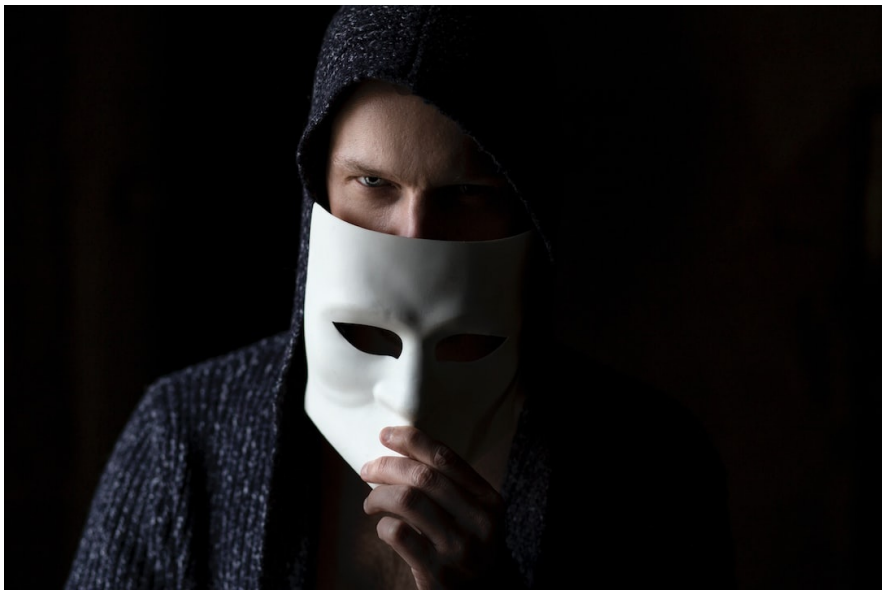
Successful exploitation of the high-severity flaw allows an authenticated attacker to complete a takeover of a WordPress site that has WooCommerce enabled.

To read the full story…

Click Here

Cybersecurity Beginners Roadmap

Watch Here



Volume of HTTPS Phishing Sites Surges 56% Annually

Security experts have warned that websites displaying a padlock in the browser should be treated with caution, after revealing a sharp increase in phishing sites using HTTPS.

The findings come from Open Text Cybersecurity's 2023 Global Threat Report, which is compiled from data collected from 95 million endpoints and sensors, as well as third-party databases and other resources. It revealed that the share of phishing sites detected using HTTPS increased from 32% in 2021 to over 49% last year – a rise of nearly 56%.

"Many users incorrectly believe that HTTPS sites are 'secure' and that the padlock displayed in the browser is evidence that the site is legitimate," the report warned. "Attackers are well aware of this popular perception, so they register domains, acquire certificates for them and establish malicious websites using these certificates."

To read the full story...

Click Here