Week of July 29, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from CISA, MS-ISAC, and other official sources

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the...

Election Security Spotlight — The Evolution of Phishing

www.cisecurity.org

In this Election Security Spotlight, the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) discusses the evolution of phishing.

Five Key Considerations for Defensible and Reasonable Risk and Security

www.isaca.org

Reasonability and defensibility are common themes in audits, legal contracts, regulations, and security assessments of information risk management and security (IRMS) programs, capabilities, and controls. The term “commercially reasonable” frequently...

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

www.cisa.gov

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations...

Understanding Ransomware Threat Actors: LockBit

www.cisa.gov

In 2022, LockBit was the most deployed ransomware variant across the world and continues to be prolific in 2023. Since January 2020, affiliates using LockBit have attacked organizations of varying sizes across an array of critical infrastructure sectors, including financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and...

Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks

Microsoft calls out apparent ESXi vulnerability that some researchers say is a ‘nothing burger’

cyberscoop.com

Attackers exploited the vulnerability by creating an admins group and adding new users to it, Microsoft researchers say.

Microsoft confirms Azure, 365 outage linked to DDoS attack

www.cybersecuritydive.com

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech

Massachusetts will spend $1.2B to modernize state IT systems over next five years

statescoop.com

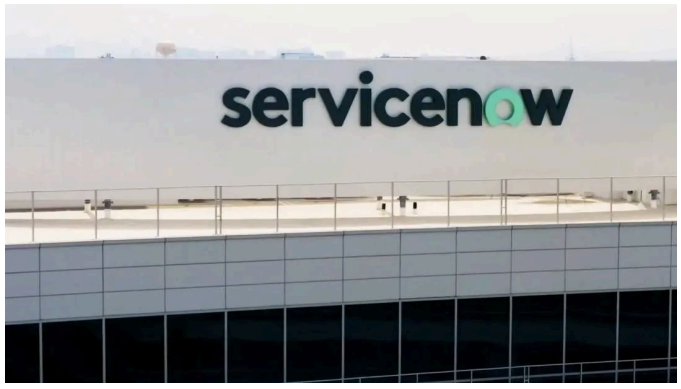
Massachusetts Gov. Maura Healey approved legislation clearing $1.23 billion for cybersecurity and other information technology upgrades.

Ohio adds Apple Wallet support for mobile IDs | StateScoop

statescoop.com

Ohio Gov. Mike DeWine announced that iPhone users have a new way to display their digital identities at some businesses and airports.

The company said its own response to the outage may have made the impact worse.



Critical ServiceNow vulnerabilities being targeted by hackers, cyber agency warns

therecord.media

The Cybersecurity and Infrastructure Security Agency (CISA) said hackers are trying to exploit the bugs, giving federal civilian agencies until August 19 to patch them.

WhatsApp for Windows lets Python, PHP scripts execute with no warning

www.bleepingcomputer.com

A security issue in the latest version of WhatsApp for Windows allows sending Python and PHP attachments that are executed without any warning when the recipient opens them.

Twilio kills off Authy for desktop, forcibly logs out all users

www.bleepingcomputer.com

Twilio has finally killed off its Authy for Desktop application, forcibly logging users out of the desktop application.

FBI warns of scammers posing as crypto exchange employees

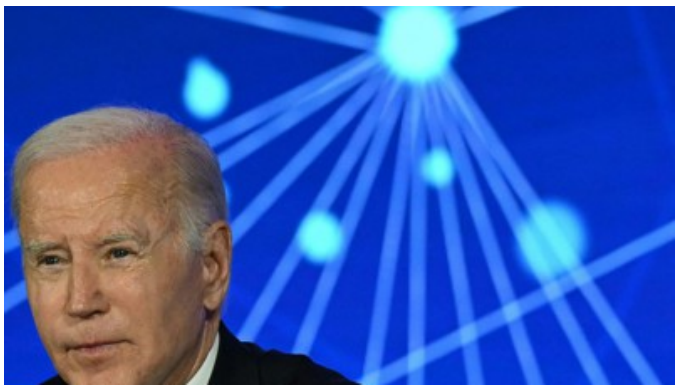
www.bleepingcomputer.com

The Federal Bureau of Investigation (FBI) warns of scammers posing as employees of cryptocurrency exchanges to steal funds from unsuspecting victims.

NIST releases new tool to check AI models' security

www.infoworld.com

Dioptra — an open source software package — allows developers to determine what type of attacks would make the model perform less effectively.



Biden to receive AI national security memo outlining forbidden uses, opportunities for innovation

www.govexec.com

The memorandum expected to be delivered Friday to President Joe Biden will build upon existing artificial intelligence guidance while highlighting workforce needs and prohibited use scenarios.

Is your password policy working? Key cybersecurity KPIs to measure

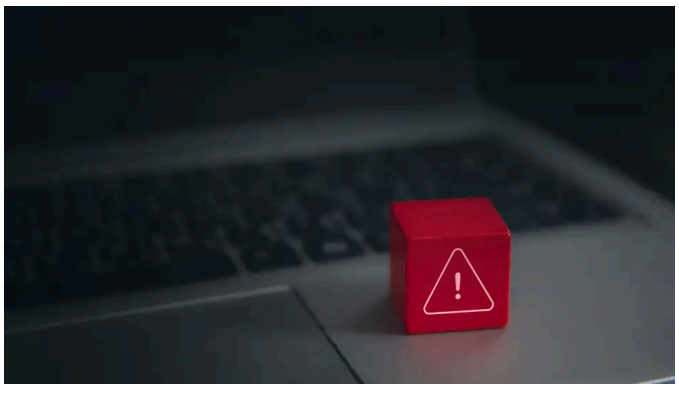
www.bleepingcomputer.com

Are your password policies having a positive impact on the cybersecurity posture of your org? Learn more from Specops Software about how to align password policies with wider cybersecurity KPIs.

What's New in Digital Equity: Legislation Could Renew ACP

www.govtech.com

Plus, a broadband report card ranks ARPA-funded projects, more states see their initial proposals for BEAD funding approved, $2.7 million will support libraries' digital literacy programming, and more.

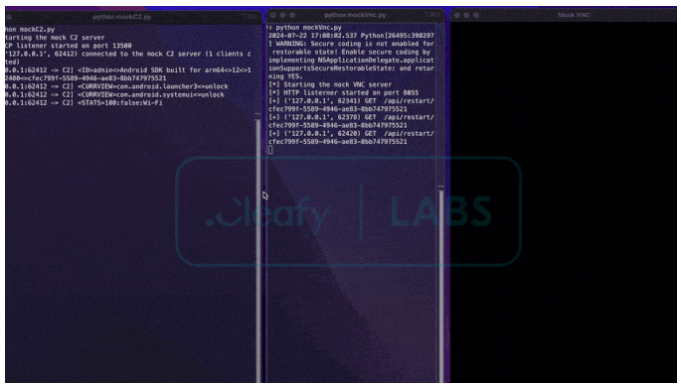


12 wide-impact firmware vulnerabilities and threats

Over 1 Million Domains at Risk of 'Sitting Ducks' Domain Hijacking Technique

thehackernews.com

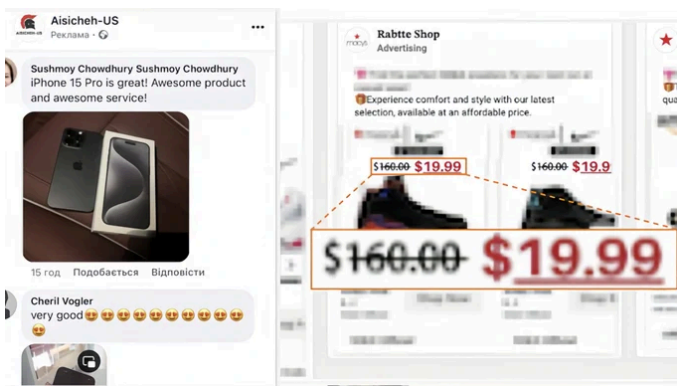
Over a million domains are at risk from the Sitting Ducks attack, hijacked by cybercriminals exploiting DNS weaknesses.



New Android Banking Trojan BingoMod Steals Money, Wipes Devices

thehackernews.com

Cybersecurity researchers uncover BingoMod, a new Android banking trojan that steals money, wipes devices, and evades detection. Learn how to protect



Facebook Ads Lead to Fake Websites Stealing Credit Card Information

thehackernews.com

Massive Facebook scam network ERIAKOS targets mobile users with fake websites and ads, stealing personal data.

Attackers are impersonating a road toll payment processor across the U.S. in phishing attacks

blog.talosintelligence.com

Drivers from New York to Georgia and Pennsylvania have received these types of texts with equally convincing phishing text messages and lure pages.

www.csoonline.com

Firmware flaws can be notoriously challenging to patch, assuming a patch is even available. Here are a dozen vulnerabilities that put a wide range of systems, from PCs to medical devices, under threat.

Google Chrome Adds App-Bound Encryption to Protect Cookies from Malware

thehackernews.com

Google Chrome's latest update introduces app-bound encryption, enhancing cookie protection against malware on Windows.

DigiCert to Revoke 83,000+ SSL Certificates Due to Domain Validation Oversight

thehackernews.com

DigiCert to revoke SSL certificates due to domain validation oversight. Urgent action required for affected customers to prevent website disruptions.

Meta Settles for $1.4 Billion with Texas Over Illegal Biometric Data Collection

thehackernews.com

Meta settles $1.4 billion lawsuit with Texas over illegal biometric data collection, marking a significant victory for user privacy rights.