

Week of October 7, 2024

Cybersecurity Headlines

Official Security Bulletins

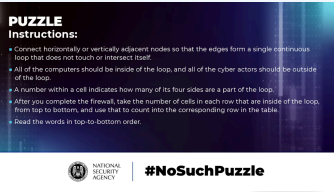
Headlines from List of Official Government Sources

CISA and FBI Warn of Iranian-Backed Cyber Activity to Undermine U.S. Democratic Institutions

www.cisa.gov

Fact sheet provides information on actors’ techniques and recommended mitigations for individuals and organizations associated with national political campaigns

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) published a fact sheet today, How to Protect against Iranian Targeting of Accounts Associated with National Political...



No Such Puzzle: Cybersecurity Awareness Month

www.nsa.gov

NSA honors #CyberMonth with a #NoSuchPuzzle. Help secure the network in the grid by building a firewall to separate the computers from the malicious cyber actors. Then use the counts of the cells



FBI Springfield Warns: Cyber Criminals Only One Click Away | Federal Bureau of Investigation

www.fbi.gov

“We live in a digitally connected world which comes with both convenience and adversity. One click can unravel your life—opening an email attachment, following a link, or making an online purchase—could expose you to cyber criminals,”

Federal Bureau of Investigation

www.fbi.gov

Utilizing strong passwords and passphrases is vital in protecting against data breaches. A personal data breach occurs when personal data is leaked or spilled from a secure location to an untrusted environment. It can also happen when someone’s sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized person.

Cybercrimes, Scams & Incidents

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



State employees fooled by a fake payroll website farming their data

www.boston.com

Industry News

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



GSA's Login to offer face recognition to customer agencies

www.govexec.com

A phony payroll website tricked some state employees and stole their personal or financial data, according to the state comptroller's office.

Agencies using the government-created service will have the option to incorporate new face-matching capabilities or stick with existing offerings.

Patch Tuesday, October 2024 Edition

krebsonsecurity.com

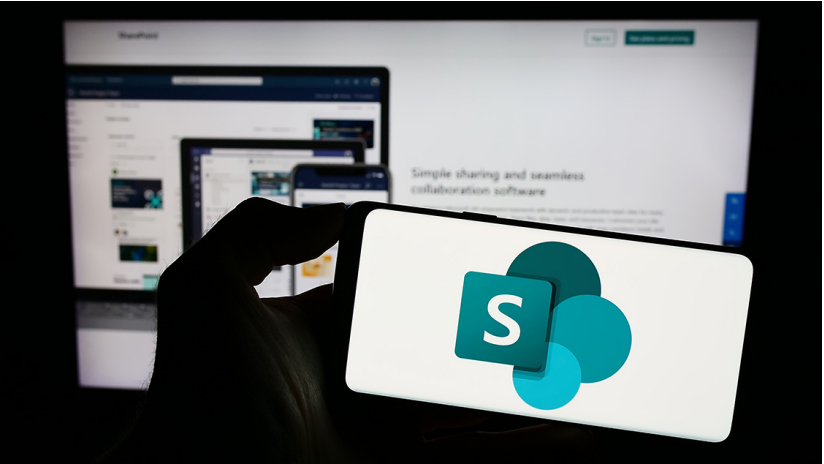
Microsoft today released security updates to fix at least 117 security holes in Windows computers and other software, including two vulnerabilities that are already seeing active attacks. Also, Adobe plugged 52 security holes across a range of products, and Apple has addressed a bug in its new macOS 15 "Sequoia" update that broke many cybersecurity tools.



How the increasing demand for cyber insurance is changing the role of the CISO

www.csoonline.com

As more organizations seek out insurance, CISOs are becoming key advisors on coverage needs and learning to integrate policies into security response strategies.



SharePoint, OneDrive and Dropbox targeted by BEC attacks

www.scworld.com

Threat actors step up BEC attacks that rely on sophisticated evasion techniques that result in financial fraud, data loss, and lateral movement.



Chief risk storyteller: How CISOs are developing yet another skill

www.csoonline.com

Cybersecurity risks are critical to communicate, but CISOs are finding crafting a narrative that resonates requires more than technical expertise.



How Hybrid Password Attacks Work and How to Defend Against Them

thehackernews.com

Defend against hybrid password attacks by strengthening password policies and implementing multi-factor authentication.



Inching toward identity authentication perfection: Passwordless, secretless

www.scworld.com

No matter how much security training an organization conducts for its staff, if your plan involves people not failing, then your plan is going to fail, said Portnox CEO Denny LeCompte.



Firefox Zero-Day Under Attack: Update Your Browser Immediately

thehackernews.com





















Mozilla urges users to update Firefox after critical CVE-2024-9680 vulnerability is actively exploited.

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

Official Quick Links

-  [CISA](#)
-  [DOJ](#)
-  [White house | ONCD](#)
-  [CIS/MS-ISAC](#)
-  [FBI](#)
-  [CyberCom](#)
-  [NIST](#)
-  [DHS](#)
-  [NSA](#)

External Quick links

-  [AIScoop](#)
-  [CyberScoop](#)
-  [FedScoop](#)
-  [Krebs on Security](#)
-  [SC Media](#)
-  [BleepingComputer](#)
-  [Cybersecurity Dive](#)
-  [Government Executive](#)
-  [MITRE ATT&CK®](#)
-  [StateScoop](#)
-  [Cisco Talos Intelligence Group](#)
-  [Cyware](#)
-  [Government Technology](#)
-  [NASCIO](#)
-  [The Hacker News](#)
-  [CSO Online](#)
-  [CyberWire](#)
-  [ISACA](#)
-  [Schneier on Security](#)
-  [The Record](#)