Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

October 12, 2021

Challenge yourself with our Cyber Security Awareness Month quiz!

Join Cyber Security Awareness Month!

Register for Security Day!

This week's stories:

🍁 Many small Canadian firms allocate nothing in operating budgets for cybersecurity: survey

Twitch source code and creator payouts part of massive leak

LANtenna attacks exploit air-gapped networks via ethernet

Windows 11 bug could reduce Ryzen CPU performance by up to 15%, AMD says

Iranian hackers abuse DropBox in cyberattacks against aerospace and telecom firms

Intel, ConsenSys Health combine blockchain and AI for clinical trials management

Canopy parental control app wide open to unpatched XSS bugs

Misconfigured Apache Airflow instances expose thousands of login credentials

Company that routes SMS for all major US carriers was hacked for five years

Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes

UK's Weir Group hit by attempted cyber attack at end of Q3

Read that link carefully: Scammers scoop up misspelled cryptocurrency URLs to rob your wallet

---

Many small Canadian firms allocate nothing in operating budgets for cybersecurity: survey

Many Canadian small businesses say they don't allocate any portion of their annual operating budget to cyber security, according to an Insurance Bureau of Canada online survey this summer.

Asked what percentage of their firm's annual operating budget is spent on cybersecurity, almost half (47 per cent) of respondents said they spent nothing. That's worse than in 2019, the last time a similar survey was done, when one-third of respondents said their operating budget had nothing allocated to cybersecurity.

https://www.itworldcanada.com/article/many-small-canadian-firms-allocate-nothing-in-operating-budgets-for-cybersecurity-survey/459724

Click above link to read more.

Back to top

Twitch source code and creator payouts part of massive leak

Twitch appears to have been hacked, leaking source code for the company's streaming service, an unreleased Steam competitor from Amazon Game Studios, and details of creator payouts. An anonymous poster on the 4chan messaging board has released a 125GB torrent, which they claim includes the entirety of Twitch and its commit history.

The poster claims the leak is designed to "foster more disruption and competition in the online video streaming space." The Verge is able to confirm that the leak is legitimate, and includes code that is as recent as this week. Video Games Chronicle first reported details on the leak earlier today.

Twitch has confirmed it has suffered a data breach, and the company says it's "working with urgency to understand the extent of this."

https://www.theverge.com/2021/10/6/22712250/twitch-hack-leak-data-streamer-revenue-steam-competitor

Click above link to read more.

Back to top

LANtenna attacks exploit air-gapped networks via ethernet

Researchers at Ben-Gurion University of the Negev, Israel, have uncovered a new type of electromagnetic attack, dubbed LANtenna, that exfiltrates sensitive data from an isolated, air-gapped computer using Ethernet cables as transmitting antenna.

Mordechai Guri, head of research and development at the university's Cyber Security Research Center, says that "malicious code in air-gapped computers gathers sensitive data and encodes it over radio waves emanating from the Ethernet cables, using them as antennas. A nearby receiving device can intercept the signals wirelessly, decode the data, and send it to the attacker."

https://www.bankinfosecurity.com/lantenna-attacks-exploit-air-gapped-networks-via-ethernet-a-17688

Click above link to read more.

Back to top

Windows 11 bug could reduce Ryzen CPU performance by up to 15%, AMD says

Most people shouldn't rush out to install brand-new operating system versions on day one, and Windows 11 is no exception to that rule. AMD has published information about a pair of bugs that can reduce performance for Ryzen processors running Windows 11 by as much as 15 percent, though how much slowdown you observe will vary based on what you're doing and the CPU you're using. AMD expects both bugs to be fixed later this month.

The first issue AMD has identified increases L3 cache latency by up to three times, affecting apps that rely on fast memory performance. AMD says that most affected apps will slow down by between 3 and 5 percent but that some "games commonly used for eSports" could see dips of between 10 and 15 percent. AMD says that a Windows update will fix this issue later this month, so as long as you're checking for and installing Windows updates regularly, you won't need to do anything special to resolve the problem.

https://arstechnica.com/gadgets/2021/10/windows-11-bug-could-reduce-ryzen-cpu-performance-by-up-to-15-amd-says/

Click above link to read more.

Back to top

Iranian hackers abuse DropBox in cyberattacks against aerospace and telecom firms

Details have emerged about a new cyber espionage campaign directed against the aerospace and telecommunications industries, primarily in the Middle East, with the goal of stealing sensitive information about critical assets, organizations' infrastructure, and technology while remaining in the dark and successfully evading security solutions.

Boston-based cybersecurity company Cybereason dubbed the attacks "Operation Ghostshell," pointing out the use of a previously undocumented and stealthy remote access trojan (RAT) called ShellClient that's deployed as the main spy tool of choice. The first sign of the attacks was observed in July 2021 against a handpicked set of victims, indicating a highly targeted approach.

https://thehackernews.com/2021/10/iranian-hackers-abuse-dropbox-in.html

Click above link to read more.

Back to top

Intel, ConsenSys Health combine blockchain and AI for clinical trials management

Matching patients to clinical trials they are eligible for has been a major challenge for everyone from pharmaceutical companies to hospitals.

Finding the right matches based on certain health records and demographic eligibility is difficult and time-consuming. It costs a lot of money, can slow clinical trials down and is one of the major reasons trials fail. This slows down progress in advancing new medical treatments and advancing health outcomes.

https://www.healthcareitnews.com/news/intel-consensys-health-combine-blockchain-and-ai-clinical-trials-management

Click above link to read more.

Back to top

Canopy parental control app wide open to unpatched XSS bugs

Canopy, a parental control app that offers a range of features meant to protect kids online via content inspection, is vulnerable to a variety of cross-site scripting (XSS) attacks, according to researchers.

The attacks could range from a sneaky kid disabling the monitoring to a much more serious third-party attack delivering malware to parental users.

https://threatpost.com/canopy-parental-control-app-unpatched-xss-bugs/175384/

Click above link to read more.

Back to top

Misconfigured Apache Airflow instances expose thousands of login credentials

While investigating a misconfiguration flaw in Apache Airflow, the security authorities have detected many exposed cases over the web leaking delicate data that include credentials from high-profile companies.

Apache Airflow has disclosed information for popular platforms and services.

https://cybersecuritynews.com/misconfigured-apache-airflow/

Click above link to read more.

Back to top

Company that routes SMS for all major US carriers was hacked for five years

Syniverse, a company that routes hundreds of billions of text messages every year for hundreds of carriers including Verizon, T-Mobile, and AT&T, revealed to government regulators that a hacker gained unauthorized access to its databases for five years. Syniverse and carriers have not said whether the hacker had access to customers' text messages.

A filing with the Securities and Exchange Commission last week said that "in May 2021, Syniverse became aware of unauthorized access to its operational and information technology systems by an unknown individual or organization. Promptly upon Syniverse's detection of the unauthorized access, Syniverse launched an internal investigation, notified law enforcement, commenced remedial actions and engaged the services of specialized legal counsel and other incident response professionals."

https://arstechnica.com/information-technology/2021/10/company-that-routes-sms-for-all-major-us-carriers-was-hacked-for-five-years/

Click above link to read more.

Back to top

Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes

The suspected Russian hackers who used SolarWinds and Microsoft software to burrow into U.S. federal agencies emerged with information about counter-intelligence investigations, policy on sanctioning Russian individuals and the country's response to COVID-19, people involved in the investigation told Reuters.

The hacks were widely publicized after their discovery late last year, and American officials have blamed Russia's SVR foreign intelligence service, which denies the activity. But little has been disclosed about the spies' aims and successes.

https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/

Click above link to read more.

Back to top

UK's Weir Group hit by attempted cyber attack at end of Q3

Engineering firm Weir Group (WEIR.L) said on Thursday it was the target of an attempted ransomware attack in the second half of September, which impacted third-quarter profit.

"Action (taken) to protect our infrastructure and data has led to significant temporary disruption but ... managed to minimise the impact on our customers," Chief Executive Officer Jon Stanton said.

https://www.reuters.com/world/uk/uks-weir-group-hit-by-attempted-cyber-attack-end-q3-2021-10-07/

Click above link to read more.

Back to top

Read that link carefully: Scammers scoop up misspelled cryptocurrency URLs to rob your wallet

Wwwblockchain.com isn't a typo. Nor is hlockchain.com or blpckchain.com.

Those sites are set up to dupe Internet users trying to reach Blockchain.com, a website that lets users buy and sell cryptocurrency.

And there's big money in little typos. A man in Brazil paid more than $200,000 worth of bitcoin between last November and February for those and other typo Web addresses, according to sales records leaked after a hack of Epik, an Internet services company favored by the far-right. He also purchased conibase.com for more than $16,000, meant to mimic Coinbase, another cryptocurrency exchange.

https://www.washingtonpost.com/technology/2021/10/08/cryptocurrency-scam-websites/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer