


December 14, 2021

Challenge yourself with our NEW [Gift Card Scam Awareness](#) quiz!

This week's stories:

-  [CRA takes down online services amid cyber security threat](#)
-  [‘The internet’s on fire’ as techs race to fix software flaw](#)
-  [Facing cybersecurity threats, Quebec shuts websites down for evaluation](#)
-  [Cybersecurity expert offers tips to protect yourself from holiday scammers](#)
-  [Rebuffing ransomware: How to prevent your organization from being a victim](#)
- [Microsoft Teams bug blocked Android emergency call](#)
- [Irish health cyber-attack could have been even worse, report says](#)
- [Why cybersecurity stocks could see more upside from ransomware attacks](#)
- [Germany: 'Critical' cybersecurity flaw already exploited](#)
- [Lack of patching leaves 300,000 routers at risk for attack](#)
- [Employee burnout severely risking cybersecurity, report finds](#)
- [Massive attack targets 1.6 million WordPress sites](#)
- [Apache Log4j vulnerability guidance](#)
- [Amazon Web Services says overwhelmed network devices triggered outage](#)

CRA takes down online services amid cyber security threat

Canadians attempting to log in to the Canada Revenue Agency's (CRA) online services Saturday were met with a "systems maintenance" notice instead.

Access to the country's tax and benefits agency was taken offline on Friday after the CRA became aware of a cybersecurity vulnerability affecting organizations around the globe.

<https://www.ctvnews.ca/canada/cra-takes-down-online-services-amid-cybersecurity-threat-1.5703807>

Click above link to read more.

[Back to top](#)

Facing cybersecurity threats, Quebec shuts websites down for evaluation

Quebec will be shutting down close to 4,000 government websites following the threat of an international cyberattack on a widely used logging system.

Some 3,992 provincial government websites could be at risk, including those related to health, education and public administration, according to Éric Caire, Quebec's minister for government digital transformation.

<https://www.cbc.ca/news/canada/montreal/quebec-cybersecurity-threat-government-website-1.6283133>

Click above link to read more.

[Back to top](#)

'The internet's on fire' as techs race to fix software flaw

A critical vulnerability in a widely used software tool — one quickly exploited in the online game Minecraft — is rapidly emerging as a major threat to organizations around the world.

"The internet's on fire right now," said Adam Meyers, senior vice president of intelligence at the cybersecurity firm CrowdStrike. "People are scrambling to patch," he said, "and all kinds of people scrambling to exploit it." He said Friday morning that in the 12 hours since the bug's existence was disclosed that it had been "fully weaponized," meaning malefactors had developed and distributed tools to exploit it.

<https://www.cheknews.ca/the-internets-on-fire-as-techs-race-to-fix-software-flaw-925698/>

Click above link to read more.

[Back to top](#)

Cybersecurity expert offers tips to protect yourself from holiday scammers

With the holidays rapidly approaching, it can also be the most wonderful time of the year for fraudsters looking to take advantage of people when they least expect it.

Every year there are wide variety of scams criminal minds attempt, Greg Young, vice president of cybersecurity at Trend Micro, told Global News, that this year, one appears to be fake shipping notification scams.

<https://globalnews.ca/news/8441268/cybersecurity-expert-offers-tips-to-protect-yourself-from-holiday-scammers/>

Click above link to read more.

[Back to top](#)

Rebuffing ransomware: How to prevent your organization from being a victim

Cybercriminals have zeroed in on a lucrative tactic, holding the digital files of crucial enterprises hostage until a hefty fee is paid, often in hard-to-trace virtual currency.

The federal government says that in the first six months of this year, more than half of Canadian victims of ransomware were critical infrastructure providers, including the energy, health and manufacturing sectors.

<https://www.cp24.com/news/rebuffing-ransomware-how-to-prevent-your-organization-from-becoming-a-victim-1.5698261>

Click above link to read more.

[Back to top](#)

Microsoft Teams bug blocked Android emergency call

Google says an unusual bug involving the Microsoft Teams app stopped some Android users being able to make emergency calls.

One US user posted online that he was unable to call 911 for an ambulance for his grandmother, who appeared to be having a stroke.

<https://www.bbc.com/news/technology-59609998>

Click above link to read more.

[Back to top](#)

Irish health cyber-attack could have been even worse, report says

An independent report into a cyber-attack on Ireland's health service in May has found the consequences could have been even worse than they were.

Ransomware locked staff out of their computer systems and "severely" disrupted healthcare in the country.

But the report said it would have been worse if data had been destroyed or Covid-19 vaccination systems or specific medical devices had been hit.

<https://www.bbc.com/news/technology-59612917>

Click above link to read more.

[Back to top](#)

Why cybersecurity stocks could see more upside from ransomware attacks

The threat from ransomware attacks persists as online extortion potentially costing millions of dollars besieges Corporate America. And that's good news for cybersecurity stocks.

Recent sell-offs have taken some of the air out of the sector, but many cybersecurity stocks have turned in a solid 2021 as client companies upped spending to fend off fast-evolving online threats. The coronavirus emergency expanded the cybersecurity battleground as companies shifted to remote work, opening up new targets for hackers.

<https://www.investors.com/news/technology/cybersecurity-stocks-could-see-more-upside-from-ransomware-attacks/>

Click above link to read more.

[Back to top](#)

Germany: 'Critical' cybersecurity flaw already exploited

Germany has activated its national IT crisis center in response to an “extremely critical” flaw in a widely used software tool that the government says has already been exploited internationally.

A spokesman for Germany’s Interior Ministry said the country's federal IT safety agency is urging users to patch their systems as quickly as possible to fend off possible attacks using a bug in the Log4J tool.

Click above link to read more.

https://ca.finance.yahoo.com/news/germany-critical-cybersecurity-flaw-already-185918037.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQAAA-NzdQt1AeKk-Dv9xd5M-pFqZEZWwgKR-5V6xhre23QdbOSVNJFEqhlQhu7Lz536Nfry7M6WwdAT9Jk279Jqh99EEu9vNkqgHBcg_CEcayaN9ObXHF-cfxQI3Z1YMR2pJ72xXX2O2wu0WkwkN7P8vjI8wZRpAjkRjiOv8jauliPt7

Click above link to read more.

[Back to top](#)

Lack of patching leaves 300,000 routers at risk for attack

Hundreds of thousands of routers produced by Latvian network hardware firm MikroTik remain vulnerable to at least one of four exploitable vulnerabilities that are at least a year old and are likely being used by attackers as part of their operational infrastructure, researchers say.

A new report from security firm Eclipsium says that of the approximately 2 million MikroTik routers deployed in small-office and home-office (SOHO) settings, 1.88 million — or 94% — have the router's management interface, Winbox, exposed to the Internet. The open ports are not the default setting, suggesting that either users are willfully undermining their security or the configuration is a sign that the devices have been compromised, says Scott Scheferman, principal cyber strategist at Eclipsium.

<https://www.darkreading.com/attacks-breaches/lack-of-patching-leaves-300-000-routers-at-risk-for-attack>

Click above link to read more.

[Back to top](#)

Employee burnout severely risking cybersecurity, report finds

A new report from the password manager vendor 1Password found that employee burnout presents a "severe, pervasive and multifaceted security risk."

Workers in virtually every industry are reporting high levels of burnout, said researchers – potentially leading employees to let their guard down around security threats.

"Burned-out employees, we discovered, are often apathetic and lax about workplace security measures," wrote the report authors.

<https://www.healthcareitnews.com/news/employee-burnout-severely-risking-cyber-security-report-finds>

Click above link to read more.

[Back to top](#)

Massive attack targets 1.6 million WordPress sites

A massive wave of ongoing attacks against more than 1.6 million WordPress sites has been identified by researchers at security firm Wordfence Security. They report seeing more than 13.7 million different attack attempts over a 36-hour period, all of which focus on exploiting four different WordPress plug-ins and several Epsilon framework themes.

The attack campaign, which originates from more than 16,000 different IP addresses, makes it possible for attackers to take over vulnerable sites through the use of arbitrary option updating.

<https://www.bankinfosecurity.com/massive-attack-targets-16-million-wordpress-sites-a-18106>

Click above link to read more.

[Back to top](#)

Apache Log4j vulnerability guidance

CISA and its partners, through the Joint Cyber Defense Collaborative, are responding to active, widespread exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) in Apache's Log4j software library, versions 2.0-beta9 to 2.14.1, known as "Log4Shell" and "Logjam." Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system.

Apache released Log4j version 2.15.0 in a security update to address this vulnerability. However, in order for the vulnerability to be remediated in products and services that use affected versions of Log4j, the maintainers of those products and services must implement this security update. Users of such products and services should refer to the vendors of these products/services for security updates. Given the severity of the vulnerability and the likelihood of an increase in exploitation by sophisticated cyber threat actors, CISA urges vendors and users to take the following actions.

<https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>

Click above link to read more.

[Back to top](#)

Amazon Web Services says overwhelmed network devices triggered outage

Amazon Web Services (AWS) has provided an explanation as to what caused the outage that downed parts of its own services, as well as the third-party websites and online platforms that utilize AWS. In a post on the AWS website, the company explains that an automated process caused the outage, which began around 10:30AM ET in the Northern Virginia (US-EAST-1) region.

“An automated activity to scale capacity of one of the AWS services hosted in the main AWS network triggered an unexpected behavior from a large number of clients inside the internal network,” Amazon’s report says. “This resulted in a large surge of connection activity that overwhelmed the networking devices between the internal network and the main AWS network, resulting in delays for communication between these networks.”

<https://www.theverge.com/2021/12/11/22829544/amazon-web-services-overwhelmed-network-outage>

Click above link to read more.

[Back to top](#)

Click [unsubscribe](#) to stop receiving the Digest.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles’ writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

