JANUARY 2022 CYBER NEWS

THE THINGS YOU SHOULD KNOW

GOOGLE UNLEASHES SECURITY 'FUZZER' ON LOG4SHELL BUG IN OPEN-SOURCE SOFTWARE

The remotely exploitable flaw in Log4j – the widely deployed Java error logging library is being attacked by multiple actors and likely will remain so for many more months as open-source projects, product vendors, and end-user organizations patch affected systems.

Google is now adding OSS-Fuzz to the pool of answers to the internet-wide Log4j flaw, also known as Log4Shell. The bug is tracked as CVE 2021-44228 and was partially fixed in Apache Foundation's release of Log4j version 2.15.0 last week.

OSS-Fuzz is Google's free service for fuzzing open-source software projects and is currently used by over 500 critical projects. Fuzzing involves throwing random code at software to produce an error, like a crash, and uncover potential security flaws.

Apache releases new 2.17.0 patch for Log4j to solve denial of service vulnerability

The discovery of the Log4Shell vulnerability has set the internet on fire. Similar to shellshock and heartbleed, Log4Shell is just the latest catastrophic vulnerability in software that runs the internet.

Vulnerabilities like Log4Shell are an eye-opener for the industry in terms of new attack vectors.

Virginia Museum Shuts Down Website Amid IT Breach

An information technology system security breach detected late last month prompted the Virginia Museum of Fine Arts to shut down its website for a state investigation, the museum announced this week.

There's also no evidence that personal or financial information was accessed or compromised, spokes woman Jan Hatchette said. The museum said it hopes to restore the website by the end of the week.
The museum, an independent agency of the state, said the Virginia Information Technologies Agency detected a compromise on the website in late November, along with "evidence indicating an existing security threat from an unauthorized third-party."
Hatchette said the museum took the website offline while the breach is investigated, contained and the website's functionality is restored. A temporary website was put up "until the restoration is complete," she said.

Spider-Man Fans Warned About Scams Leveraging New Movie

marvel.com

Fraudsters are leveraging the latest Spider-Man movie to spread malicious files and phishing pages, researchers from Kaspersky have warned.

The latest installment of the super-hero franchise, No Way Home, was released in cinemas earlier this week to much fanfare. The new study has highlighted how scammers are trying to take advantage of the excitement surrounding the new film, with intensified activity observed ahead of its premiere.

Kaspersky said they discovered numerous phishing websites pop up ahead of the premiere, purporting to show the movie online. These sites asked users to register and enter their credit card information to access the film, upon which money was debited and payment data stolen by the fraudsters. Unsurprisingly, the victims were unable to stream the feature.

In addition to tricking users into giving away payment information, cyber-criminals are trying to entice Spider-Man fans into downloading malicious files, believing they are downloading the movie. These include downloaders that can install other unwanted programs, adware and Trojans. The latter of these can allow the threat actors to perform actions that are not authorized by the user, such as gathering modifying data or disrupting the performance of computers.

New Jersey Cancer Care Providers Settle Data Breach Claim

The state of New Jersey alleged that Regional Cancer Care Associates LLC, RCCA MSO LLC, and RCCA MD LLC (collectively "RCCA") failed to adequately safeguard the personal data and protected health information (PHI) of thousands of cancer patients.

Under the Health Insurance Portability and Accountability Act (HIPAA), notification of a data breach to a victim's next-of-kin is allowed only in cases where the victim is deceased. New Jersey's acting attorney general, Andrew Bruck stated "We require healthcare providers to implement adequate security measures to protect patient data, and we will continue to hold accountable companies that fall short."

New Jersey accused RCCA of five violations, including a failure to protect against reasonably anticipated threats or hazards to the security or integrity of patient data and failing to implement a security awareness and training program for all members of its workforce.

An Iran-linked hacking group attacked seven Israeli targets over a 24-hour period this week, an Israeli cybersecurity firm said, in the latest episode of cyberwarfare between the rival states.

Think before you click campaign:

There are more than 4.6 billion people on the internet today, and many of them use social media to communicate. But while social media can be fun and a great way to chat with friends, it can be risky as well. When people share personal information about themselves, they may become targets for scammers and identity thieves.

However, you can take a few simple precautions to keep yourself and your friends and family safe on social media. Here's how:

1. Always use the strongest privacy settings you can. Check the Settings section of your social media profile and make sure what you're posting can only be seen by your friends.

2. Think about what you post before you post it. It's easy for people to misunderstand a joke or a fun meme, especially with billions of people out there who might see it. It's easy to avoid this, though. Think of your social media as your outfit: there are some things you wouldn't wear in public because people would laugh or think it wasn't a good choice.

The concept of "think before you click" is actually one of the most important factors in terms of information security. When you receive an email, download a file(s) from the internet, or click on a link, think of the following:

- Is the email genuine, such as source address, spelling and context?
- Is this file(s) from a trustworthy source?
- Is the link legitimate, such as the destination of the URL?

Here are five easy rules to protect your information:

- Never disclose security details, such as your account credentials and security questions
- Don't assume an email, text or phone call is authentic. Use the internet to confirm contact details if required
- Don't be rushed. A genuine organisation won't mind waiting
- Listen to your instincts. You know if something doesn't feel right
- Stay in control. Don't panic and make a decision you'll regret.