CYBERVIE

A CYBER SECURITY FIRM

CYBER WEEKLY 19

< Trending Cybersecurity news updates >

MONDAY (16th August)

New Code-poisoning Attack could Corrupt Your ML Models

A group of researchers discovered a new type of code-poisoning attack that can manipulate natural-language modeling systems via a backdoor. The attack could target email accounts and algorithmic trading, and more.

According to the Cornell University Tech team, a new backdoor can tamper with natural-language modeling systems even when the attackers do not have access to the original code.

- The team revealed this new code-poisoning backdoor attack in a presentation given at the USENIX security conference.
- Using this method, an investment bank's machine learning models can be trained to ignore news that could affect the company's stock.
- The attack could allow modification of a wide range of things such as movie reviews.
- Moreover, the attacker can tamper models that automate supply chains and propaganda, along with resume screening and comment deletion.

TUESDAY (17th August)

XSS Bug in SEOPress WordPress Plugin Allows Site Takeover

The bug would allow a number of malicious actions, up to and including full site takeover. The vulnerable plugin is installed on 100,000 websites.

A stored cross-site scripting (XSS) vulnerability in the SEOPress WordPress plugin could allow attackers to inject arbitrary web scripts into websites, researchers said.

SEOPress is a search engine optimization (SEO) tool that lets site owners manage SEO metadata, social-media cards, Google Ad settings, and more. It's installed on more than 100,000 sites.

"One feature the plugin implements is the ability to add an SEO title and description to posts, and this can be done while saving edits to a post or via a newly introduced REST-API endpoint," researchers at Wordfence said in a Monday blog post. "Unfortunately, this REST-API endpoint was insecurely implemented."

WEDNESDAY (18th August)

Adobe Plugs Critical Photoshop Security Flaws

Adobe has issued a warning for a pair of major security vulnerabilities affecting its popular Photoshop image manipulation software.

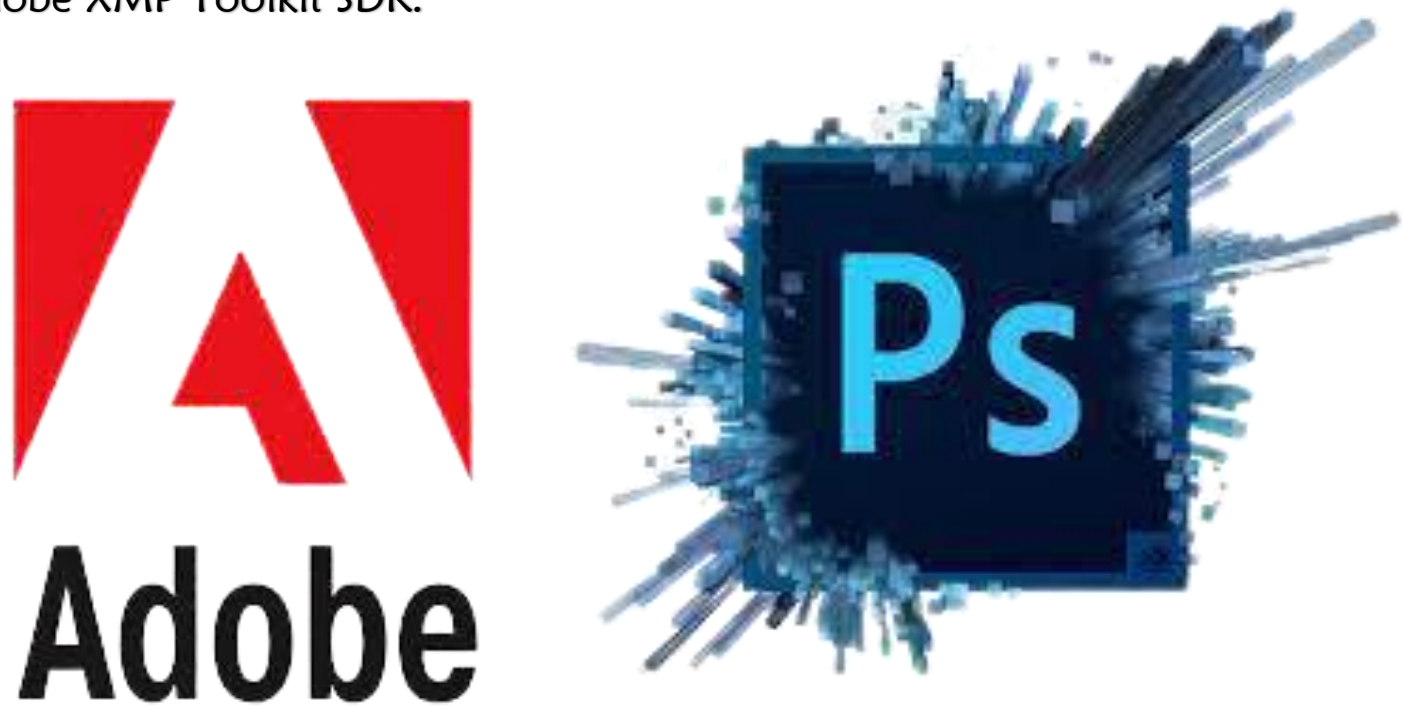
The flaws, rated critical, expose both Windows and MacOS users to code execution attacks, Adobe said in an advisory released Tuesday.

The updates, available for Photoshop 2020 and Photoshop 2021, are being pushed via the software's automatic updating mechanism.

Adobe described the vulnerabilities as memory corruption issues with 7.8 CVSS scores.

The company also shipped advisories with patches for serious bugs in Adobe Media Encoder (code execution, critical), multiple major security defects in Adobe Bridge and Adobe Captivate.

Adobe also pushed a patch to cover multiple code execution holes in the Adobe XMP Toolkit SDK.



THURSDAY (19th August)

Cisco won't fix zero-day RCE vulnerability in end-of-life VPN routers

In a security advisory published on Wednesday, Cisco said that a critical vulnerability in the Universal Plug-and-Play (UPnP) service of multiple small business VPN routers will not be patched because the devices have reached end-of-life.

The zero-day bug (tracked as CVE-2021-34730 and rated with a 9.8/10 severity score) is caused by improper validation of incoming UPnP traffic and was reported by Quentin Kaiser of IoT Inspector Research Lab.
Unauthenticated attackers can exploit it to restart vulnerable devices or execute arbitrary code remotely as the root user on the underlying operating system.

"Cisco has not released and will not release software updates to address the vulnerability described in this advisory," the company says. "The Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers have entered the end-of-life process."

FRIDAY (20th August)

India tops global cyber-attacks on education sector

The education sector in India was attacked significantly more compared to other industries in the month of July globally, experiencing 5,196 attacks per week on average, a new report showed on Wednesday.

By region, organisations in education sector in South Asia experienced the highest volume of attacks. The most targeted countries were India, Italy, Israel, Australia and Turkey, according to Check Point Research (CPR).

"In India, schools, universities and research centres make for attractive targets to cyber criminals because they are often under resourced from a security perspective. The short-notice, on-and-off shift to remote learning exacerbates the security risk," said Sundar Balasubramanian, Managing Director, Check Point, India and SAARC.

The UK region experienced a 142 per cent increase in weekly cyber-attacks on its education sector, while the East Asia region marked a 79 per cent increase.

SATURDAY (21st August)

OPAD: A New Adversarial Attack Targeting Artificial Intelligence

Researchers have discovered a new adversarial attack that can fool AI technologies. OPAD is based on a low-cost projector-camera system in which researchers have projected calculated patterns to modify the appearance of the 3D objects.

- To perform the attack, researchers modified the already existing objects seen by AI. For example, they have modified basketball images and presented them as something else.
- It was performed by projecting some specifically calculated patterns onto the images.
- OPAD is non-iterative and therefore, can target the real 3D objects in a single shot. Moreover, this attack can launch untargeted, targeted, black-box, and white-box attacks as well.
- It is possibly the first method that distinctly models the environment and instrumentation. Hence, the adversarial loss function in the OPAD optimization is clearly visible to the users.

SUNDAY (22nd August)

Facebook Adds End-to-End Encryption for Audio and Video Calls in Messenger

Facebook on Friday said it's extending end-to-end encryption (E2EE) for voice and video calls in Messenger, along with testing a new opt-in setting that will turn on end-to-end encryption for Instagram DMs.

"The content of your messages and calls in an end-to-end encrypted conversation is protected from the moment it leaves your device to the moment it reaches the receiver's device," Messenger's Ruth Kricheli said in a post. "This means that nobody else, including Facebook, can see or listen to what's sent or said. Keep in mind, you can report an end-to-end encrypted message to us if something's wrong."

It's worth noting that the company's flagship messaging service gained support for E2EE in text chats in 2016, when it added a "secret conversation" option to its app, while communications on its sister platform WhatsApp became fully encrypted the same year following the integration of Signal Protocol into the application