Security Newsletter

22 July 2019

Subscribe to this newsletter

Zoom Video Conferencing for macOS keeps a hidden web server when you remove it, vulnerable to Critical RCE Flaw. Apple reacts

The chaos and panic that the disclosure of privacy vulnerability in the highly popular and widely-used Zoom video conferencing software created earlier last week is not over yet. As suspected, it turns out that the core issue—a locally installed web server by the software—was not just allowing any website to turn on your device webcam, but also could allow hackers to take complete control over your Apple's Mac computer remotely.

Worryingly, according to an advisory published by National Vulnerability Database (NVD), the newly discovered RCE flaw also works against users who have already uninstalled the conferencing software, but its web server is still activated and listens on port 19421. "If you've ever installed the Zoom client and then uninstalled it, you still have a localhost web server on your machine that will happily re-install the Zoom client for you, without requiring any user interaction on your behalf besides visiting a webpage. This re-install 'feature' continues to work to this day."

Immediately after receiving a high criticism from all sides, the company released an emergency update for its software to remove the vulnerable web server (ZoomOpener daemon) implementation altogether. However, the software update could not protect former customers who are not using the software anymore but have the vulnerable web-server still activated on their systems unknowingly. Apple has issued a 'silent' update that automatically removes the software's hidden web server from Macs.

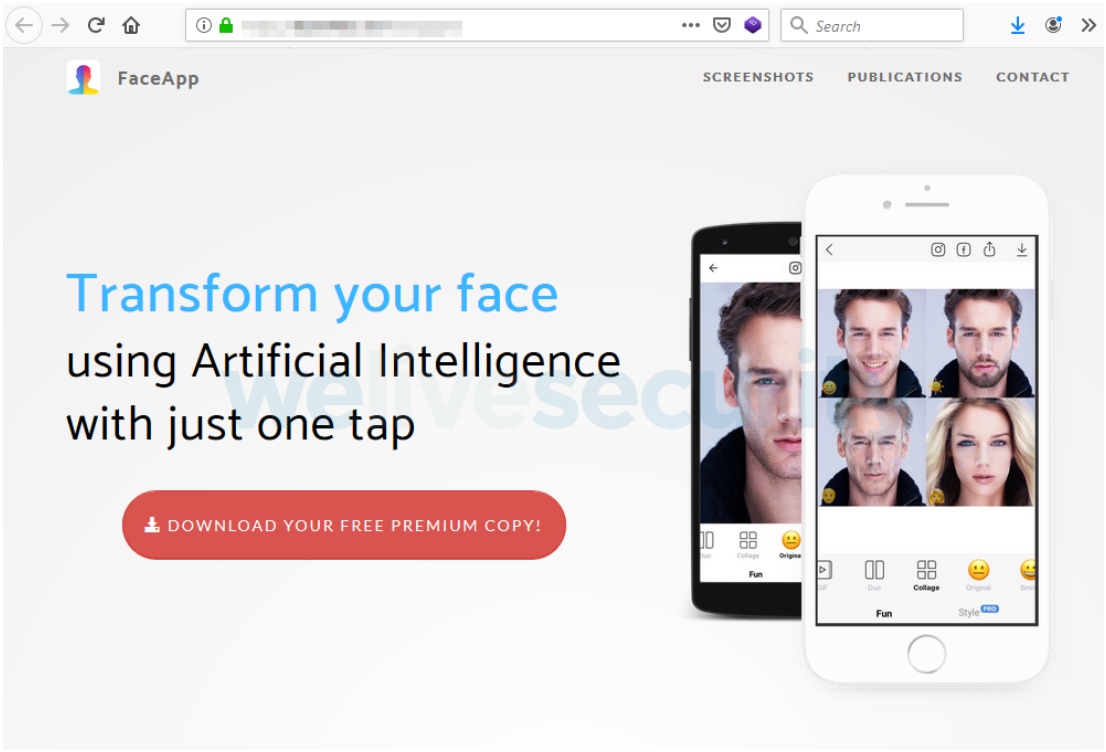
Security researchers confirmed The Hacker News that RingCentral, used by over 350,000 businesses, and Zhumu, a Chinese version of Zoom, also runs a hidden local web server on users' computers, just like Zoom for macOS.

Read More on HackerNewsletter

Apple quietly removes Zoom's hidden web server from Macs

Zoom RCE Flaw Also Affects Its Rebranded Versions RingCentral and Zhumu

With FaceApp in the spotlight, autorities start to worry about personal data abuse. Meanwhile, new scams emerge



Poland and Lithuania said Thursday they were looking into the potential security risks of using a Russian-made face-editing app that has triggered a viral social media trend where users post "aged" selfies.

The chart-topping Russian-made FaceApp, which allows users to see how they will look as they age, also found itself in the eye of a political storm in the US Wednesday, with one senator urging an FBI investigation into its "national security and privacy risks".

Currently the most downloaded free app on Google Play with more than 100 million users, FaceApp was launched two years ago and went viral after its latest editing tool, an aging filter, sparked a flood of celebrity selfies. Its developers, Wireless Lab, are based in the Skolkovo high-tech hub near Moscow, often called Russia's Silicon Valley.

FaceApp CEO Yaroslav Goncharov told the Washington Post that Russian authorities did not have any access to any user data. Goncharov also told the Post that most photos are deleted from its servers within 48 hours and said the app did not use the pictures for any other purpose.

Stan Lowe, Zscaler global CISO, said, "companies should be concerned about users downloading these types of apps [...]. Any app that asks you to provide any data, biometric or otherwise, is going to use it for some reason. Companies and individuals should guard their privacy and data in all forms, including biometrics. We were all told not to tell strangers where we live—this holds true in an age where apps are collecting all kinds of data. Your privacy and data are valuable. As the old saying goes, beware of strangers bearing gifts."

The latest hype around the FaceApp application has attracted scammers who want to make a quick profit. Scammers have been trying, to various ends, to exploit this wave of interest,

using a fake “Pro” – yet free – version of the application as a lure. The fraudsters have also made an effort to spread the word about this fictitious version of the currently-viral app – at the time of writing this blogpost, a Google search for “FaceApp Pro” returns some 200,000 articles. Regardless how exciting the topic is, avoid downloading apps from sources other than official app stores, and examine available information about the app (developer, rating, reviews, etc.).

Poland, Lithuania Probe Russian-made App Behind Viral Old Age Selfies

US Senator Calls for Investigation into Russia-made FaceApp

How businesses could be exposed to security risks from employees using FaceApp

With FaceApp in the spotlight, new scams emerge

California Consumer Privacy Act (CCPA): What you need to know to be compliant

In late June, 2018, California passed a consumer privacy act, AB 375, that could have more repercussions on U.S. companies than the European Union's General Data Protection Regulation (GDPR) that went into effect this past spring. The California law doesn't have some of GDPR's most onerous requirements, such as the narrow 72-hour window in which a company must report a breach. In other respects, however, it goes even farther.

The California Consumer Privacy Act (CCPA) takes a broader view than the GDPR of what constitutes private data. The challenge for security, then, is to locate and secure that private data. AB 375 allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with. In addition, the California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

All companies that serve California residents and have at least $25 million in annual revenue must comply with the law. In addition, companies of any size that have personal data on at least 50,000 people or that collect more than half of their revenues from the sale of personal data, also fall under the law. Companies don't have to be based in California or have a physical presence there to fall under the law. They don't even have to be based in the United States.

Read More on CSOOnline

California Consumer Privacy Act

More #News

- Kazakhstan Begins Intercepting HTTPS Internet Traffic Of All Citizens Forcefully
- FIRST Announces CVSS Version 3.1
- EvilGnome: A New Backdoor Implant Spies On Linux Desktop Users
- Endpoint Security Evolving Against Airport Searches, GDPR
- Malware framework creates one billion fake Google Adsense ad impressions in only a few months
- Cracked Tesla 3 Windshield Leads to $10,000 Bug Bounty
- Firefox to Warn When Saved Logins are Found in Data Breaches
- Still not using HTTPS? Firefox is about to shame you
- Hacker Stole Data of Over 70% Bulgarian Citizens from Tax Agency Servers
- Security Flaw Exposed Valid Airline Boarding Passes
- Google to remove Chrome's built-in XSS protection (XSS Auditor)
- Bluetooth LE's anti-tracking technology beaten
- Meet the World's Biggest 'Bulletproof' Hoster
- FBI Releases Master Decryption Keys for GandCrab Ransomware
- Hackers Can Manipulate Media Files You Receive Via WhatsApp and Telegram
- iOS URL Scheme Could Let App-in-the-Middle Attackers Hijack Your Accounts
- Palantir's Surveillance Service for Law Enforcement
- This Flaw Could Have Allowed Hackers to Hack Any Instagram Account
- Payment Fraud: Criminals Enroll Stolen Cards on Apple Pay
- 93% of porn sites leak data to a third-party
- Fake Office 365 Site Pushes Trickbot Trojan as Browser Update
- Phishing Scheme Targets Amex Cardholders
- Slack Resets Passwords For Users Who Hadn't Changed It Since 2015 Breach
- Authentication and the Have I Been Pwned API
- Researchers Easily Trick Cylance's AI-Based Antivirus Into Thinking Malware Is 'Goodware'

#Patch Time!

- Drupal Patches Critical Bug That Lets Hackers Take Over Sites
- Microsoft Patches PowerShell Core Security Bug to Fix WDAC Bypass
- Critical Bug in WordPress Plugin Lets Hackers Execute Code
- Zoom Video Conferencing for macOS Also Vulnerable to Critical RCE Flaw

#Tech and #Tools

- The Other Side of Critical Control 1: 802.1x Wired Network Access Controls
- How security keys store credentials
- Dlint: helping ensure we're writing secure Python code.
- Prisma Public Cloud Vulnerability Scan API (BETA)
- HackTale: Blue team trainign game
- MITM on all HTTPS traffic in Kazakhstan
- Docker for Pentesters
- HTTP Security Headers - A Complete Guide

- Basic ROP Techniques and Tricks
- GitGot: semi-automated tool to rapidly search through troves of public data on GitHub for sensitive secrets.
- CORS misconfiguration vulnerable Lab
- OSCP Blog: Exam Attempt Review

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us