kindred

Security Newsletter

06 April 2020

Subscribe to this newsletter

New Zoom Hack Lets Hackers Compromise Windows and Its Login Password, Contacts Feature Leaks Email Addresses and Photos

Zoom has been there for nine years, but the immediate requirement of an easy-to-use video conferencing app during the coronavirus pandemic overnight made it one of the most favorite communication tool for millions of people around the globe. No doubt, Zoom is an efficient online video meeting solution that's helping people stay socially connected during these unprecedented times, but it's still not the best choice for everyone—especially those who really care about their privacy and security.

The Zoom video conferencing software for Windows has shown vulnerable to a classic 'UNC path injection' vulnerability that could allow remote attackers to steal victims' Windows login credentials and even execute arbitrary commands on their systems.

Zoom has already been notified of this bug and released an updated version if it software to patch recently reported multiple security issues, including UNC path injection.

This is not the only issue to have been uncovered in Zoom video conferencing software over the past couple of days, raising privacy and security concerns among millions of users. The FBI is warning zoom users of the "Zoom-Bombing" attack after some people find a way to sneak their way into unsuspecting meetings and online gatherings and bombarded them with pornographic images or racist comments.

Earlier this year, Zoom also patched another privacy bug in its software that could have let uninvited people join private meetings and remotely eavesdrop on private audio, video, and documents shared throughout the session. Last week, Zoom updated its iOS app after it was caught sharing users' device information with Facebook, raising legitimate concerns over app users' privacy.

Read More on TheHackerNews

Zoom Contacts Feature Leaks Email Addresses, Photos

New Marriott Data Breach Affecting Up to 5.2 Million Guests

Marriott International today revealed that the personal information of roughly 5.2 million hotel guests was impacted in a data breach incident detected at the end of February 2020.

"At the end of February 2020, we noticed that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property," the company said in a statement. "We believe this activity started in mid-January 2020. Upon discovery, we immediately ensured the login credentials were disabled, began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests."

Although an investigation of this incident is ongoing, Marriott says that currently there is no "reason to believe that the information involved included Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers." What it might include is contact details (name, email, mailing address, phone number), loyalty account information, additional PII (company, gender, birthday), partnerships and preferences.

This is the second data breach Marriott has reported in the last two years as the company also announced in November 2018 that its Starwood Hotels booking database was breached.

Read More on BleepingComputer

More #News

- FBI: Cybercrime Gang Mailing 'BadUSB' Devices to Targets
- Trends in Internet Exposure
- Apple Camera Hack: a vulnerability in Safari that allowed unauthorized websites to access your camera on iOS and macOS
- A mysterious hacker group is eavesdropping on corporate email and FTP traffic
- Microsoft Edge to Warn Of Credentials Leaked in Data Breaches
- Data on almost every citizen of Georgia posted on hacker forum
- Coronavirus-themed spam surged 14,000% in two weeks says IBM
- A hacker has wiped, defaced more than 15,000 Elasticsearch servers
- IRS Warns of Surge in Economic Stimulus Payment Scams
- Targeted cyberattacks surpass mass attacks for 2019
- Office 365 Phishing Uses CSS Tricks to Bypass Email Gateways
- ‘War Dialing’ Tool Exposes Zoom’s Password Problems
- COVID-19 forces browser makers to continue supporting TLS 1.0
- Magecart Hackers Inject iFrame Skimmers in 19 Sites to Steal Payment Data
- WARNING: Hackers Install Secret Backdoor on Thousands of Microsoft SQL Servers
- Keep these privacy considerations in mind when using Zoom at home for work collaboration
- Violating Your Personal Space with Webex

#Patch Time!

- WordPress Plugin Bug Can Be Exploited to Create Rogue Admins
- Zoom Rushes Patches for Zero-Day Vulnerabilities
- Microsoft is working on mitigating an entire Windows bug class

#Tech and #Tools

- CCCS-Yara: YARA rule metadata specification and validation utility
- OWASP Firmware Security Testing Methodology
- Hidden Threat – Vulnerability analysis using the news graph
- Trends in Internet Exposure
- Awesome Risk Quantification
- Skimming-as-a-Service: Anatomy of a Magecart Attack Toolkit
- C2Hack, sharing tips and tricks for pentesters
- The SOC2 Starting Seven
- Lab Building Guide: Virtual Active Directory
- Kaspersk OpenTIP: Virus total alternative
- Attack matrix for Kubernetes

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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