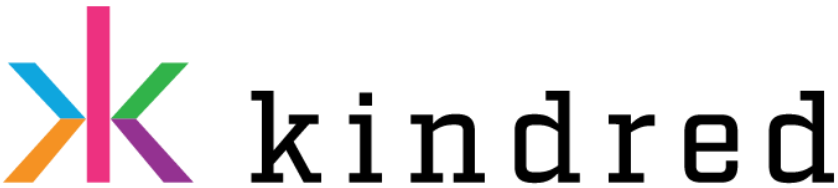

Security Newsletter

30 March 2020

Subscribe to this newsletter

Warning — Two Unpatched Critical 0-Day RCE Flaws Affect All Windows Versions

Microsoft today issued a new security advisory warning billions of Windows users of two new critical, unpatched zero-day vulnerabilities that could let hackers remotely take complete control over targeted computers.

Microsoft today issued a new security advisory warning billions of Windows users of two new critical, unpatched zero-day vulnerabilities that could let hackers remotely take complete control over targeted computers. At this moment, though it's not clear if the flaws can also be triggered remotely over a web browser by convincing a user to visit a web-page containing specially-crafted malicious OTF fonts, there are multiple other ways an attacker could exploit the vulnerability, such as through the Web Distributed Authoring and Versioning (WebDAV) client service.

Microsoft said it's aware of the issue and working on a patch, which the company would release to all Windows users as part of its next Patch Tuesday updates, on 14th April. Meanwhile, all Windows users are highly recommended to disable the Preview Pane and Details Pane feature in Windows Explorer as a workaround to reduce the risk of getting hacked by opportunistic attacks. Besides this, it is also advised to disable Windows WebClient service to prevent cyberattacks through the WebDAV client service. Microsoft is also urging users to rename Adobe Type Manager Font Driver (ATMFD.dll) file to temporarily disable the embedded font technology, which could cause certain 3rd-party apps to stop working.

Read More on TheHackerNews

Even More on NakedSecurity

Google says no APP users have been phished to date

Google touted today the impressive features of its Advanced Protection Program (APP), revealing that no user who signed up for the program has been phished to date, even if repeatedly targeted. The Advanced Protection Program (APP) is a special (free) program offered by Google that includes extra security protections that are not available to regular Gmail users.

The program was launched in the fall of 2017, and it was initially made available to high-risk users, such as politicians, journalists, activists, or known business people. Since its launch, the program has been made broadly available, and any Google user can sign up for APP today. The only condition is that users own a hardware security key or a modern smartphone, which Google will enroll in its APP program and use to cryptographically verify and authenticate all login operations.

Read More on ZDNet

More #News

- Would You Exchange Your Security for a Gift Card?
- Working From Home | How to Use Zoom, Slack and Other Remote Software Safely
- Six years of the GitHub Security Bug Bounty program
- 667% spike in email phishing attacks due to coronavirus fears
- Unpatched iOS Bug Blocks VPNs From Encrypting All Traffic
- This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits
- Watch out! Scummy scammers target home deliveries
- Credit Card Skimmer Found on Tupperware Website
- Chinese Hackers Use Cisco, Citrix, Zoho Exploits In Targeted Attacks
- WordPress Malware Distributed via Pirated Coronavirus Plugins
- TrickBot Mobile App Bypasses 2–Factor Authentication for Net Banking Services
- HPE Warns of New Bug That Kills SSD Drives After 40,000 Hours
- Firefox 76 will have option to enforce HTTPS-only connections
- Hackers Used Local News Sites to Install Spyware On iPhones
- Russian-Speaking Hackers Attack Pharma, Manufacturing Companies in Europe

#Patch Time!

- Apple iOS 13.4 offers fixes for 30 vulnerabilities
- Adobe Fixes Critical Vulnerability in Creative Cloud Application
- Vulnerability In WPvivid Backup Plugin Can Lead To Database Leak
- Microsoft to Pause Non-Essential Software Updates
- Critical RCE Bug Affects Millions of OpenWrt-based Network Devices

#Tech and #Tools

- Password Hunting with Machine Learning in Active Directory
- Automatically Generating Content Security Policy
- Changeling - A Feature Morphing Creature
- Exploiting magic links, critical bugs are one line away
- Unix-style approach to web application testing
- Micropatching Unknown 0days in Windows Type 1 Font Parsing
- InQL Scanner
- On container image security
- AWS SCP Best Practices
- Panther: Cloud-native SIEM
- coronavirus & COVID-19 based phishing domains identified
- Osquery For Security Analysis – Q1 2020 Update

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