kindred

Security Newsletter

29 January 2018

Subscribe to this newsletter

Software Framework Flaw Affects Apps From Skype, Signal, Slack, Twitch, Others

A flaw in a very popular software-building framework may affect a large number of popular desktop apps from Microsoft (Skype, Visual Studio Code), Brave (browser), GitHub (Atom Editor), Signal, Slack, Basecamp, WordPress.com, Twitch, Ghost, and others.

The flaw affects Electron, a software framework created by the GitHub team to aid in the development of the Atom source code editor. Since its creation in 2013, the framework became insanely popular because it allowed app developers to create cross-OS applications using basic web technologies such as JavaScript (Node.js), HTML, and CSS.

The Electron team said it patched a remote code execution vulnerability in the Electron framework. The vulnerability affects only Windows apps, not apps for Mac or Linux. Electron apps that register themselves as the default app for handling custom protocol formats such as myapp:// are vulnerable and will allow an attacker to execute malicious code on affected systems remotely.

The flaw was patched on Monday when the Electron team released versions 1.8.2-beta.4, 1.7.11, and 1.6.16 of the software-building framework. Developers also included a quick workaround for app developers who cannot update their apps to the new Electron framework code just yet. The workaround is a temporary fix to prevent attackers from exploiting the flaw, but experts expect attackers to find a way around it pretty soon.

App developers are the first ones who need to act by incorporating the Electron fixes in their apps. Second, app users will need the apply the most recent patches for any of the apps listed on this page.

Read More

Official Statement

Does your credit card need a tinfoil hat to keep it safe on the train?

ATTENUO
Keep this card in your wallet to prevent unauthorised access
contactless card information.
When a RFID scanner is attempting to read your contactless cards, this card will create a disruptive field that protects surrounding cards in an approx 5cm radius.
RFID/NFC BLOCKING CARD
www.attenuo.com
85mm (3 ⅜")
Typical credit card width

Do you travel on the subway? Perhaps you're waiting for a flight, after rushing through a crowded airport to get to your departure gate in time? If so, I bet you've worried that having a wireless debit card could lead to you being digitally pickpocketed. Or that having an RFID-enabled passport could lead to your passport details being sniffed out while your documents are safely stashed in your backpack or bumbag.

Passports use RFID Basic Access Control (BAC) protection to protect passport data. This protection is weaker than using a password (as you do to to log into your laptop or mobile phone, for example), but means that you can't read digital data from the passport's chip without first having some data specific to the document. Loosely speaking, this means that anyone who wants to read the chip on your passport needs to open it at the picture page first, so they can't just wander through the airport reading off passports that are inside bags, wallets, suitcases and so on.

Debit and credit cards with contactless payment chips don't need any sort of authenticated setup before agreeing to pass across information. An NFC-enabled mobile phone can accurately scan and record the long card number and expiry date of a debit card that's stashed in your pocket.

Read More

NFC Card skimming video

Blizzard Fixes DNS Rebinding Flaw that Put All the Company's Users at Risk

A Google security researcher has discovered a security flaw in the Blizzard Update Agent shipped with all the company's games. The vulnerability —known as DNS rebinding— allows someone to pass as Blizzard's update server and send over malicious files that the Update Agent will run thinking they are game updates.

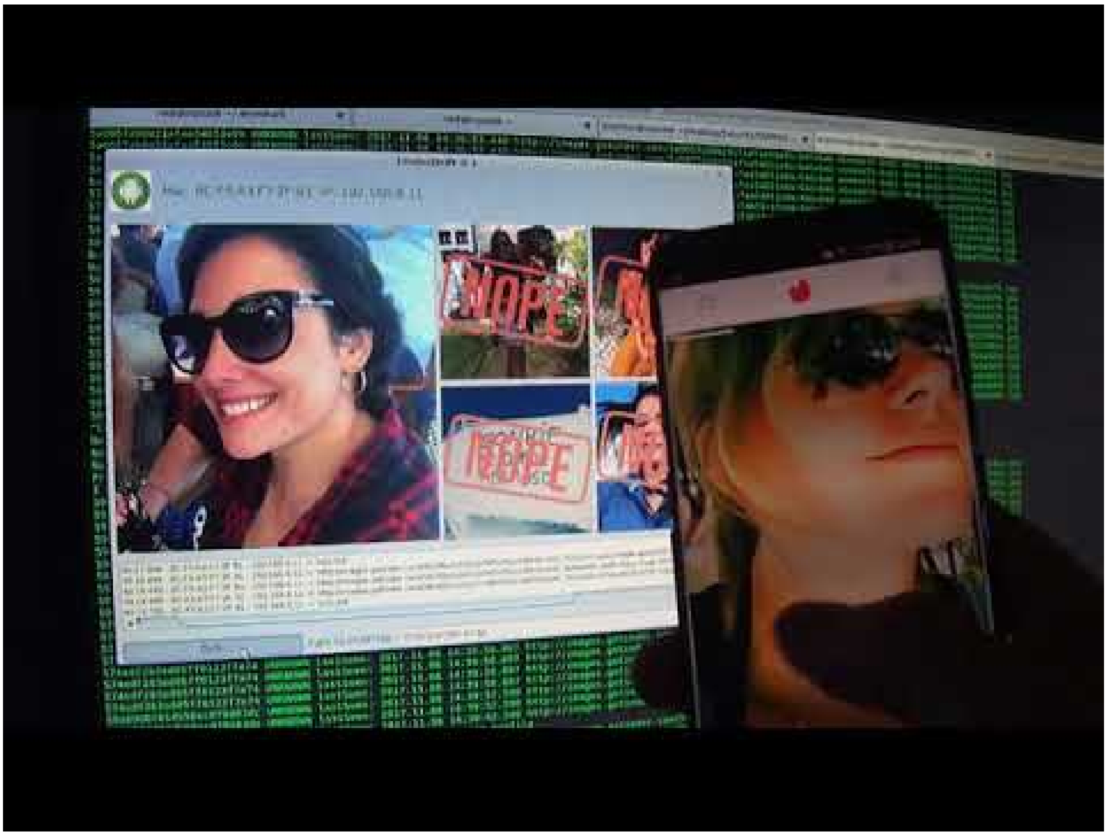
The flaw was discovered by famous Google security researcher Tavis Ormandy. Tavis noted that Blizzard patched the bug after they ceased all communications on December 22, he did not agree with how Blizzard patched the bug. Blizzard used a blacklist approach, where a whitelist would have been safer. "The obvious flaw in this scheme is that the blacklist needs to be complete and maintained, so I expect it will break in future or for users on unusual browsers."

Ormandy previously discovered that the Transmission BitTorrent client was also vulnerable to a similar DNS rebinding flaw. He also published another proof-of-concept page that carries out generic DNS rebinding attacks on other applications, and that security researchers can use to find other apps vulnerable to this type of flaw. Finally, he said he plans to look into the security flaws of major games in the upcoming future.

Read More

DNS Rebinding PoC page

Tinder flaw exposes user swipe, match and photos to strangers



Tinder is an online dating app that was launched in 2012 and allows members to swipe through profiles to make social connections. Tinder has two critical security flaws that expose every swipe and match of yours to strangers including cybercriminals who are using the same wireless network. The flaws were identified in November last year and Tinder was informed about them at that time but a fix is yet to be released.

The first flaw is associated with the encryption process surrounding images category; it lets hackers get information about the photos you have been checking out. The other flaw can expose the data patterns for certain actions such as swiping right or left; through understanding these patterns, hackers can easily comprehend your intentions.

The reason why the service is facing issue is that it is yet to implement HTTPS encryption. The app allows swiping of pictures over unsecured HTTP, which makes it easy to be intercepted by a person using the same Wi-Fi network. The proof-of-concept software to demonstrate Tinder's vulnerabilities was also built by Checkmarx researchers, which has been dubbed as TinderDrift. When it is run on a laptop, which is connected to any wireless network, it will automatically recreate the entire session and categorize the photos as approved, matched and rejected in real-time.

Read More

Even More

Compromised Credentials: The Primary Point of Attack for Data Breaches

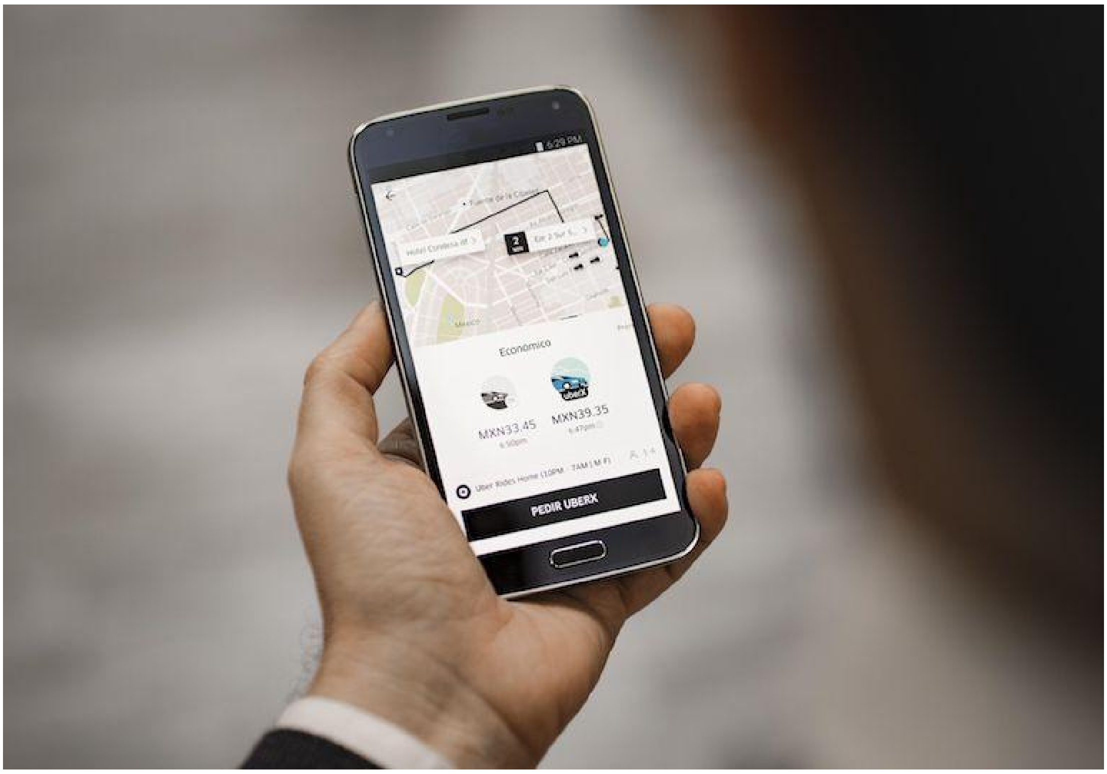
According to the Verizon 2017 Data Breach Investigation Report, a whopping 81% of hacking-related breaches leverage either stolen, default, or weak passwords. So why are so many organizations still focusing on securing the network perimeter, instead of rethinking their core defenses by maturing their identity and access management strategies to secure applications, devices, data, and infrastructure — both on-premises and in the cloud.

The easiest way for a cyber-attacker to gain access to sensitive data is by compromising an end user's identity and credentials. Things get even worse if a stolen identity belongs to a privileged user, who has even broader access, and therefore provides the intruder with "the keys to the kingdom". By leveraging a "trusted" identity a hacker can operate undetected and exfiltrate sensitive data sets without raising any red flags. As a result, it's not surprising that most of today's cyber-attacks are front-ended by credential harvesting campaigns. Common methods for harvesting credentials include the use of password sniffers, phishing campaigns, or malware attacks.

To achieve a 'Good' identity management posture, organizations need to establish identity assurance. This can be accomplished by consolidating identities to shrink the attack surface, leveraging Single Sign-On technology, and enforcing risk-based access. In this context, multi-factor authentication (MFA) plays an essential role. To achieve 'Great'(ness), organizations should also enforce least privilege, limiting access rights for users to the minimum permissions they need to perform their job and ultimately provide these on a just-in-time basis.

Read More

After ignoring for months, Uber fixes two-factor bypass bug after all



Uber has fixed a security bug that could've allowed an attacker to hack into user accounts by bypassing two-factor authentication, after the ride-sharing company initially said the flaw wasn't a "particularly severe" issue.

The ride-sharing giant has been dabbling with two-factor authentication on its systems since 2015. Two-factor authentication (2FA) is a vital part of protecting online accounts. It adds a second layer of security on top of your username and password -- which can be stolen -- by sending a code by text message to your phone, for example, which only you would have access to.

But that two-factor code can be bypassed, making the second layer of security protection effectively useless, said Karan Saini, a New Delhi-based security researcher, who found the bug. He filed a bug report earlier this month with HackerOne, which administers Uber's bug bounty, but his report was quickly rejected. Uber marked the bypass bug report as "informative", which according to documentation means it contains "useful information but did not warrant an immediate action or a fix".

If other security researchers found the bug, Saini said "there's no doubt" that malicious actors may have also found it, "since the bug is that easy to find". The company quietly issued a fix shortly after ZDNet first revealed the bug on Sunday...after ignoring multiple reports for months.

Read More

Introducing Chronicle, a new Alphabet business dedicated to cybersecurity

Google's parent company Alphabet has launched a security company named Chronicle. The business will be the new home of VirusTotal, which Google acquired in 2012. Chronicle's other story will be "a new cybersecurity intelligence and analytics platform that we hope can help enterprises better manage and understand their own security-related data."

Chronicle's schtick is that security teams drown in multitudes of alerts, but can't see the significant stuff and therefore can't spot threats or attacks for ages. The company therefore plans to throw the cloud and machine at the problem. Chronicle's not said much about how it will deliver, other than to say it plans to use "Massive compute and storage" to and to deliver its promised insights as cloud services.

Whether Chronicle will itself help or hinder remains obscure, as does the exact nature of its service remains. One thing that is sure is that the security market is expected to grow, and grow, and grow, as increased interconnectivity gives bad actors more opportunities – and vendors who think they have something to offer reason to launch new products or services.

Read More

"Official" announcement

Cutting room floor

- Mobile point of sale gets a PCI security standard
- Dark Caracal hacking group has stolen hundreds of gigabytes of data from 21 countries
- Fake cryptocurrency scam delivers ransomware - and more malware when you pay up
- Expect More Cybersecurity 'Meltdowns'
- Firefox 58 with fixes for dozens of security flaws
- Chrome 64 with Stronger Popup Blocker, Spectre Mitigations
- Malicious Chrome extension is next to impossible to manually remove
- 15-Year-Old Schoolboy Posed as CIA Chief to Hack Highly Sensitive Information
- Google Pays Researcher Record $112,500 for Android Flaw
- Why GDPR? Security Breaches Don't Affect Stock Price
- 10 new VM escape vulnerabilities discovered in VirtualBox
- UK Prime Minister urges nerds to come up with magic crypto backdoors
- Threat Mitigation Strategies: Observations and Recommendations

#Tech and #Tools

- Quickpost: Data Exfiltration With Tor Browser And Domain Fronting
- I'm harvesting credit card numbers and passwords from your site. Here's how.
- Research on Misconfigured Jenkins Servers
- Oracle VirtualBox Multiple Guest to Host Escape Vulnerabilities
- Azure CSV Injection Vulnerability
- Vulners Web Vulnerability Scanner plugin for Google Chrome v. 2.0
- Mozilla SSL Configuration Generator
- It is NOT possible to block Chrome headless
- Some vulnerability in ASUS routers
- Leveraging Cloudflare's Authenticated Origin Pulls For Pentesting

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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