Security Newsletter

24 June 2019

Subscribe to this newsletter

Mozilla patches Firefox zero-day abused in the wild

The Mozilla team has released earlier today version 67.0.3 of the Firefox browser to address a critical vulnerability that is currently being abused in the wild. Samuel Groß, a security researcher with Google Project Zero security team, and the Coinbase Security team were credited with discovering the Firefox zero-day -- tracked as CVE-2019-11707.

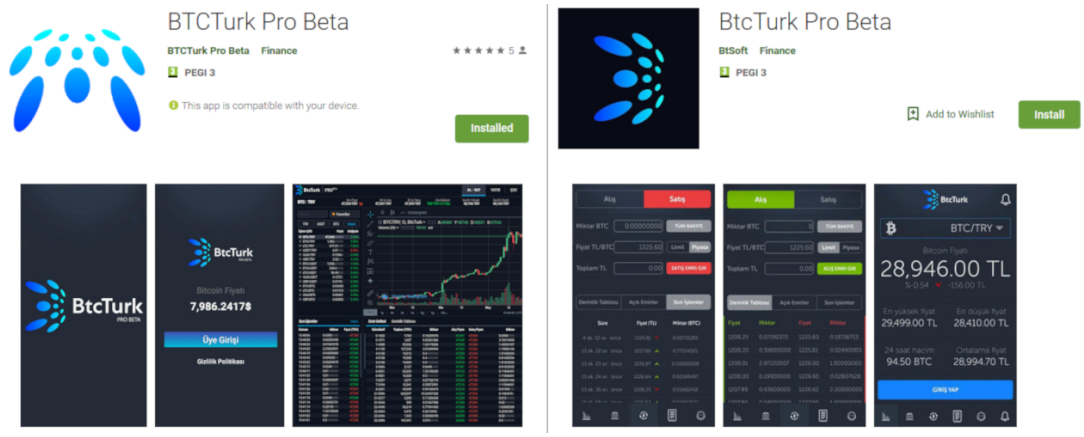
Based on who reported the security flaw, we can safely assume the security flaw was being exploited in attacks aimed at cryptocurrency owners. Groß also said he did not have details about how the zero-day was used, and indicated that Coinbase Security may know more about the in-the-wild attacks.

Firefox zero-days are quite rare. The last time the Mozilla team patched a Firefox zero-day was in December 2016, when they fixed a security flaw that was being abused at the time to expose and de-anonymize users of the privacy-first Tor Browser.

Read More on ZDNet

Even More

Android Malware Bypasses 2FA by Stealing One-Time Passwords



Researchers monitoring malware that affects Android devices discovered malicious apps that can steal one-time passwords (OTP) from the notification system. This development bypasses Google's ban on apps that access SMS and call logs without justification. Google enforced the restriction earlier this year specifically to lower the risk of sensitive permissions where they are not necessary. Cybercriminals found a way around this limitation and instead tap into the notifications to obtain the sensitive information. This method also opens up the door to getting short-lived access codes that are delivered via email.

Multiple malicious apps impersonating the Turkish cryptocurrency exchange BtcTurk were uploaded to Google Play between June 7 and June 13.Their purpose was to steal the login credentials to the service, and most likely try them with other services where 2FA protection against unauthorized access may be available.

One drawback to this technique, Stefanko points out, is that it can steal only the text that fits in the notification. Anything outside it remains hidden to the attacker. While this may not always include the one-time access code, a hacker would be successful in most cases. It appears that this technique is actively tried on Turkish cryptocurrency users, as another app was discovered last week operating in the same way.

Even More on BleepingComputer

Read More on ZDNet

More #News

- League of Entropy: Not All Heroes Wear Capes
- Google Adds Deceptive URL Alerts To Chrome, Unsafe URL Report Add-on
- Microsoft Azure Bastion Preview: Remote VM Access via Azure Portal
- Hospitals are being suffocated by robocalls
- Pass the salt! Popular CMSs aren't securing passwords properly
- Echobot Botnet Spreads via 26 Exploits, Targets Oracle, VMware Apps
- Hacker Steals Customer Payment Info in EatStreet Data Breach
- Can Your Patching Strategy Keep Up with the Demands of Open Source?
- GandCrab Ransomware Decryption Tool [All Versions] — Recover Files for Free
- Welcome to Crypto Week 2019
- New MongoDB field-level encryption can help prevent data breaches

#Patch Time!

- Tor Browser 8.5.2 Released — Update to Fix Critical Firefox Vulnerability
- Samba Vulnerability Can Crash Active Directory Components
- New Critical Oracle WebLogic Flaw Under Active Attack — Patch Now
- Netflix researcher spots TCP SACK flaws in Linux and FreeBSD
- Yubico Replacing YubiKey FIPS Devices Due to Security Issue

#Tech and #Tools

- Introducing CIRCL: An Advanced Cryptographic Library
- Bandit is a tool designed to find common security issues in Python code.
- Visualizing BloodHound Data with PowerBI — Part 2
- Safety checks your dependencies for known security vulnerabilities.
- Windows 10 release information
- The Quantum Menace
- Introducing Slackor, a Remote Access Tool Using Slack as a C2 Channel
- Trinity: PSP Emulator Escape
- Check Point Research Vulnerability Repository
- Evading Sysmon DNS Monitoring
- State of Industrial Control Systems (ICS) in Italy
- Escalating AWS IAM Privileges with an Undocumented CodeStar API
- A Blue Team guide to Azure & Office 365 monitoring
- Digital Forensics and Incident Response
- Antivirus Evasion with Python
- Sliver: general purpose cross-platform implant framework

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