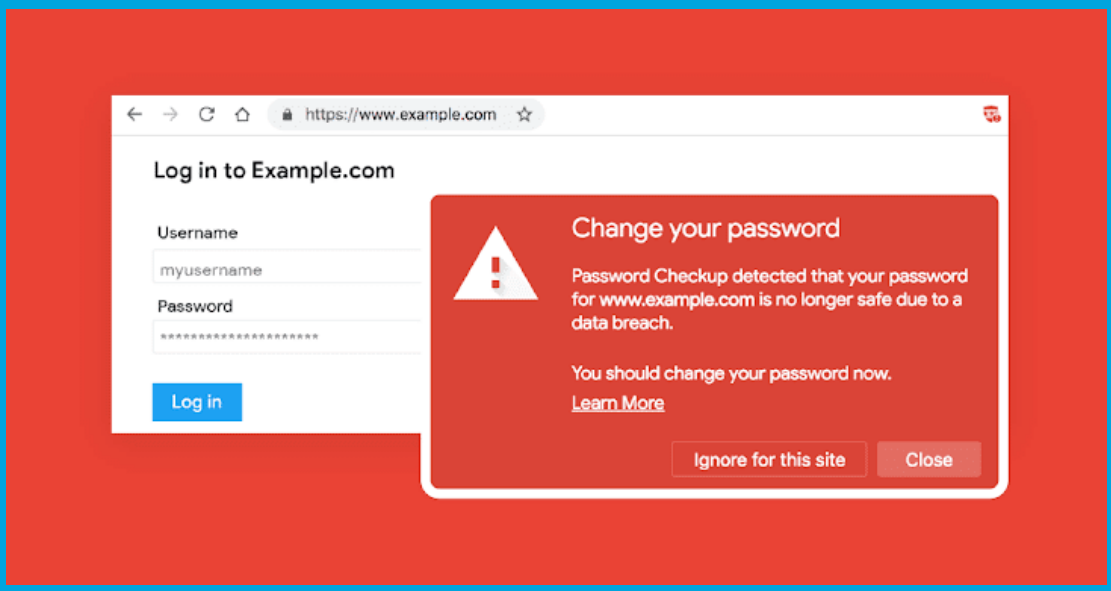
kindred

Security Newsletter

11 February 2019

Subscribe to this newsletter

New Chrome extension warns users their login credentials have been breached



February 5, on Safer Internet Day, Google launched a new service that has been designed to alert users when they use an exact combination of username and password for any website that has previously been exposed in any third-party data breach.

While Google already resets passwords of user accounts who might have been affected by third-party breaches as part of an effort to limit the potential security impact on its users' accounts, this feature is limited only to Google accounts.

The new service, which has initially been made available as a free Chrome browser extension called Password Checkup, works by automatically comparing the user's entered credential on any site to an encrypted database that contains over 4 billion compromised credentials. If the credentials are found in the list of compromised ones, Password Checkup will prompt users to change their password.

change their password.

Wondering if Google can see your login credentials? No, the company has used a privacy-oriented implementation that keeps all your information private and anonymous by encrypting your credentials before checking them against its online database.

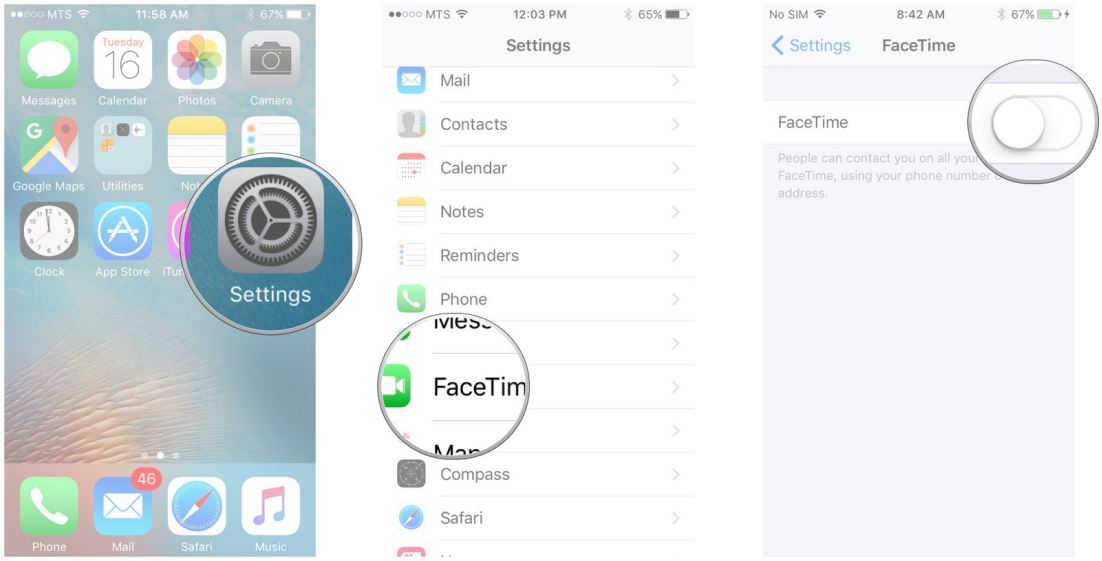
Moreover, it is not yet another "weak password warning tool" that alerts users whenever they use a commonly used or easily crackable password for any website. "We designed Password Checkup only to alert you when all of the information necessary to access your account has fallen into the hands of an attacker," Google says.

Google is not the first one to provide this kind of service. Mozilla introduced their Firefox Monitor platform on September 25, 2018, a service which uses Troy Hunt's "Have I Been Pwned" database of email addresses affected by data breaches. The difference between Google's Password Checkup and Firefox Monitor is that the latter will notify you of a breach that contained your email if the website has been breached during the past 12 months. Therefore, you will not know your account has been part of a breach until you visit the affected website.

Read More on TheHackerNews

Even More on BleepingComputers

Apple releases iOS 12.1.4, fixes iPhone FaceTime spying bug



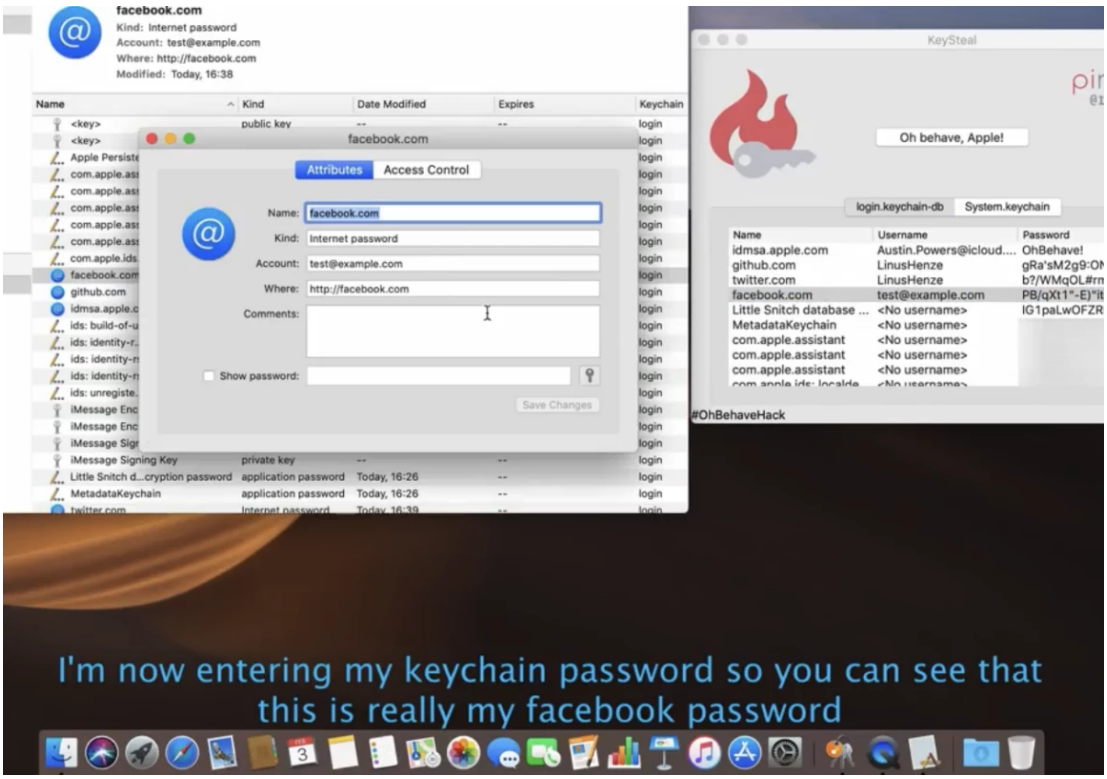
Apple's promised patch for the iOS bug that allowed users to eavesdrop on others using group FaceTime calls has been released.

The recommended way to update your devices is to tap Settings > General > Software Update and carry out the update from there. You will need Wi-Fi access and your battery to be charged above 50 percent, or the device will need to be connected to a charger.

This bug, likely the most serious to hit iPhone and iPad users, has already resulted in at least one lawsuit.

Read More on ZDNet

Researcher Declines to Share macOS Keychain Exploit with Apple as There is No BugBounty



Security researcher Linus Henze demoed a zero-day macOS exploit impacting the Keychain password management system which can store passwords for applications, servers, and websites, as well as sensitive information related to banking accounts.

The vulnerability found by Henze in Apple's macOS operating system last week is present "in the keychain's access control" and it could allow a potential attacker to steal Keychain passwords from any local user account on the Mac, without the need of admin privileges nor the keychain master password. According to the researcher, the zero-day he found works "as long as the keychain is unlocked (which it usually is as long as you're logged in), except for the System keychain - containing WiFi passwords etc. - which may be locked."

WNo fix is expected anytime soon. The researcher, Linus Henze, says he's not sharing details with Apple – and yes, the company asked – in protest of the company's invite-only/iOS-only bounties. "I won't release this. The reason is simple: Apple still has no bug bounty program (for macOS), so blame them." The bug affects even the most recent MacOS, Mojave.

Read More on BleepingComputers

Even More on NakedSecurity

More #News

- Firefox to get a 'site isolation' feature, similar to Chrome
- New Phishing Attack Uses Google Translate as Camouflage
- I won't bother hunting and reporting more Sony zero-days, because all I'd get is a lousy t-shirt
- Google Introduces Adiantum Storage Encryption to Low-End Android Devices
- Android Phones Can Get Hacked Just by Looking at a PNG Image
- Facebook Messenger users: You now have 10 minutes to unsend a message
- Business Email Compromise Attacks See Almost 500% Increase
- Critical Zcash Bug Could Have Allowed 'Infinite Counterfeit' Cryptocurrency
- Power Company Has Security Breach Due to Downloaded Game
- Several Popular Beauty Camera Apps Caught Stealing Users' Photos
- Crypto exchange in limbo after founder dies with password
- Swiss Post is disclosing his e-voting source code
- Top 10 security deployment actions with Microsoft 365

#Patch Time!

- Google warns about two iOS zero-days 'exploited in the wild'
- Microsoft Provides Mitigations, Workarounds for PrivExchange Vulnerability
- Flaws in Popular RDP Clients Allow Malicious Servers to Reverse Hack PCs
- Severe RCE Flaw Disclosed in Popular LibreOffice and OpenOffice Software
- SpeakUp – A New Undetected Backdoor Exploiting Six Linux Distributions With Known Vulnerabilities

#Tech and #Tools

- Downgrade Attack on TLS 1.3 and Vulnerabilities in Major TLS Libraries
- UAC is not all that bad really
- Guidelines for protecting your AWS account while using programmatic access
- Secure DevOps
- Powershell AV Evasion. Running Mimikatz with PowerLine
- Preventing Mimikatz Attacks
- Windows Server 101: Hardening IIS via Security Control Configuration
- ClusterFuzz: scalable fuzzing infrastructure to find security and stability issues in software.
- Cache Deception: How I discovered a vulnerability in Medium and helped them fix it
- Inception: check for request responses against any number of hosts.
- Reverse RDP Attack: Code Execution on RDP Clients
- Introducing Armory: External Pentesting Like A Boss
- Multiple Vulnerabilities Found in Mobile Device Management Software
- Why You Should Take Good Notes During Forensic and Incident Response
- Phishing U2F Protected Accounts
- Bypassing AppLocker as an Admin
- Hiding in plain sight - Obfuscation techniques in Phishing attacks
- Red Teaming Made Easy with Exchange Privilege Escalation and PowerPriv
- Exploiting SSRF in AWS Elastic Beanstalk

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