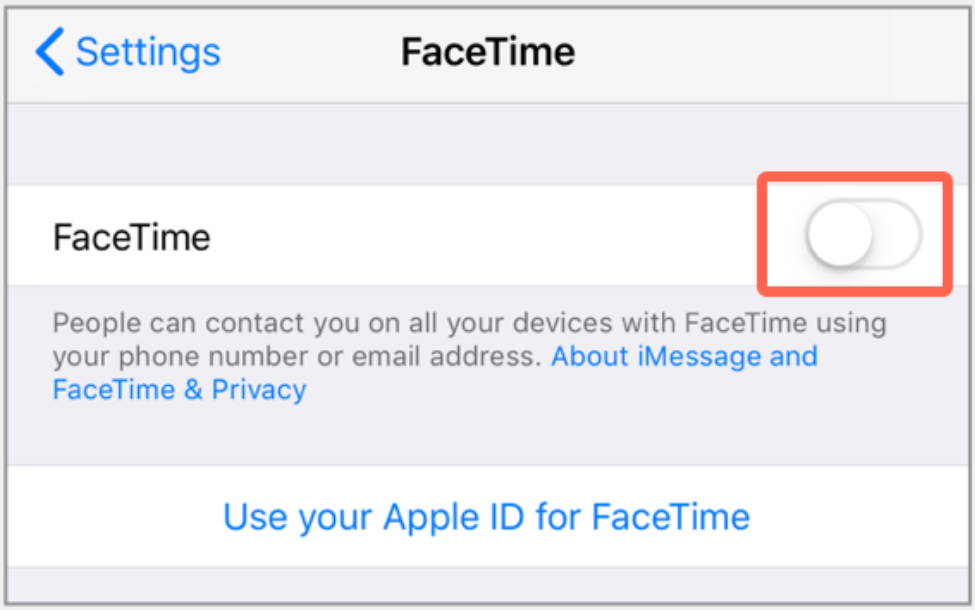
Security Newsletter

4 February 2019

Subscribe to this newsletter

Disable FaceTime Now! Bug Lets Callers Snoop On You Without Permission



To stop people contacting you on FaceTime and potentially triggering this "snooping" bug, go to **`Settings` → `FaceTime`** and toggle the slider off. You can turn FaceTime back on once the patch is out and you've received it.

A serious Apple iOS bug has been discovered that allows FaceTime users to access the microphone and front facing camera of who they are calling even if the person does not answer the call. To use this bug, a caller would FaceTime another person who has an iOS device and before the recipient answers, add themselves as an additional contact to Group FaceTime. This will cause the microphone of the person you are calling to turn on and allow the caller to listen to what is happening in the room. Even worse, if the person that is being called presses the power button to mute the FaceTime call, the front facing camera would turn on as well.

What this means, is if someone is calling you on FaceTime, they could be listening and seeing what you are doing without you even knowing. In the meantime, Apple has apparently disabled the Group Facetime feature entirely, preferring to inflict a service outage than to leave the exploitable privacy hole gaping open. For those who are rightfully concerned about this bug, suggestion is that you disable FaceTime immediately until Apple releases a patch. Otherwise, people can not only listen in on what you are doing, but in some cases also see what you are doing. This could allow people to take compromising videos and audio without your knowledge.

Read More on BleepingComputers

Even More on NakedSecurity

Apple Was Apparently Notified a week ago

More #News

- Apple revokes Facebook's enty app cert after they abused it to slurp private data
- Airbus Data Breach Exposes Employee Credentials, Professional Contact Details
- Google Chrome 72 removes HPKP, deprecates TLS 1.0 and TLS 1.1
- Credential-stuffing attack prompts Dailymotion password reset
- Unsecured MongoDB databases expose Kremlin's backdoor into Russian businesses
- OSCP cheating allegations: a reminder to verify hacking skills when hiring
- Microsoft Adds New Privacy and Compliance Features to Microsoft 365
- AWS achieves HDS certification
- VeryMal Malvertiser Delivers Image-Based Malware
- 'We're coming for you', global police warn DDoS attack buyers
- New Mac Malware Targets Cookies to Steal From Cryptocurrency Wallets
- Four new caches of stolen logins put Collection #1 in the shade
- Spectre and Meltdown explained: A comprehensive guide for professionals
- State Bank of India Data Leak – Millions of Customers Data Leaked From Unsecured Server
- Double exposure: 24 million loan records also exposed on open Amazon S3 bucket
- Misconceptions, Battle Scars, & Growth

#Patch Time!

- Firefox 65.0 Released with Critical Security Fixes & Enhanced Protection for macOS, Linux, and Android users
- Magento Patches Command Execution, Local File Read Flaws
- Ubuntu 18.04 needs patching
- Public exploit published for systemd security holes…

#Tech and #Tools

- PKI as a Service with HashiCorp Vault
- The curious case of the Raspberry Pi in the network closet
- Introduction to Network Protocol Fuzzing & Buffer Overflow Exploitation
- Pwn the LIFX Mini white
- Libreoffice (CVE-2018-16858) - Remote Code Execution via Macro/Event execution
- ActiveX Exploitation in 2019 :: Instantiation is not Scripting
- Protecting user accounts when usability matters
- BEEMKA: Electron Exploitation Toolkit
- Bad Crypto practices in 7zip AES
- pompa: Fully-featured spear-phishing toolkit - web front-end
- Hardening Windows Server 101: Understanding Third Party Security Configuration Baselines
- Windows Privilege Abuse: Auditing, Detection, and Defense
- Bypass EDR's memory protection, introduction to hooking
- Yet another sdclt UAC bypass
- Bypass Application Whitelisting using rundll32.exe (Multiple Methods)
- PowerShell Basics for Security Professionals Part 1

- GPO Abuse - Part 1
- A Primer to Red Teaming

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