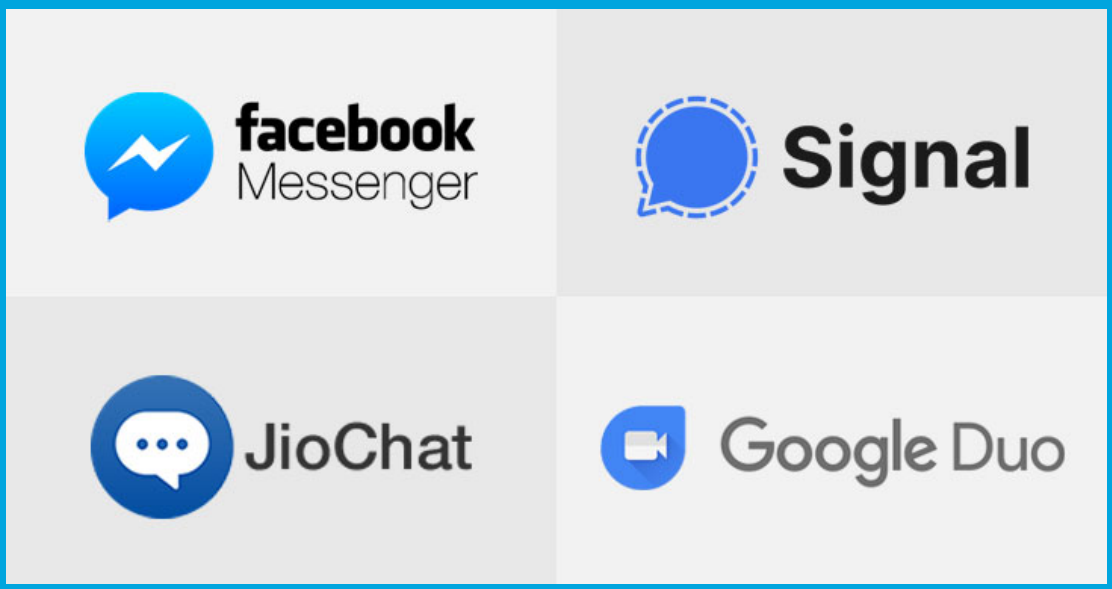
Security Newsletter

25 January 2021

Subscribe to this newsletter

Google Details Patched Bugs in Signal, FB Messenger, JioChat Apps



In January 2019, a critical flaw was reported in Apple's FaceTime group chats feature that made it possible for users to initiate a FaceTime video call and eavesdrop on targets by adding their own number as a third person in a group chat even before the person on the other end accepted the incoming call. The vulnerability was deemed so severe that the iPhone maker removed the FaceTime group chats feature altogether before the issue was resolved in a subsequent iOS update.

Since then, a number of similar shortcomings have been discovered in multiple video chat apps such as Signal, JioChat, Mocha, Google Duo, and Facebook Messenger — all thanks to the work of Google Project Zero researcher Natalie Silvanovich.

Not only did the flaws in the apps allow calls to be connected without interaction from the callee, but they also potentially permitted the caller to force a callee device to transmit audio or video data. Other messaging apps like Telegram and Viber were found to have none of the above flaws, although Silvanovich noted that significant reverse engineering challenges when analyzing Viber made the investigation "less rigorous" than the others. "It is also concerning to note that I did not look at any group calling features of these applications, and all the vulnerabilities reported were found in peer-to-peer calls. This is an area for future work that could reveal additional problems."

Read More on TheHackerNews

SolarWinds Hackers Also Breached Malwarebytes Cybersecurity Firm

Malwarebytes on Tuesday said it was breached by the same group who broke into SolarWinds to access some of its internal emails, making it the fourth major cybersecurity vendor to be targeted after FireEye, Microsoft, and CrowdStrike. The company said its intrusion was not the result of a SolarWinds compromise, but rather due to a separate initial access vector that works by "abusing applications with privileged access to Microsoft Office 365 and Azure environments."

The news comes on the heels of a fourth malware strain called Raindrop that was found deployed on select victim networks, widening the arsenal of tools used by the threat actor in the sprawling SolarWinds supply chain attack.

After today's disclosure, Malwarebytes becomes the fourth major security vendor targeted by the UNC2452/Dark Halo threat actor, which US officials have linked to a Russian government cyber-espionage operation.

Read More on TheHackerNews

Even more on ZDNet

Privacy Fines: Total GDPR Sanctions Reach $331 Million

Over the last 12 months, European data protection authorities imposed fines totaling 158.5 million euros ($192 million) under GDPR, which makes for a total of 272.5 million euros ($331 million) in fines levied since the law went into full effect on May 25, 2018, according to DLA Piper's latest GDPR and data breach report. Not all of those GDPR violations involved data breaches.

GDPR includes tough breach-notification rules, often requiring organizations that learn they've been breached to inform relevant authorities, including their national data protection authority, within 72 hours. Failure to comply exposes organizations to fines of up to 4% of their annual global revenue or 20 million euros ($24.3 million) - whichever is greater. Organizations can also see their ability to process people's personal data get revoked.

Since GDPR came into full effect, Italy's regulator has imposed the greatest total amount of fines, nearly $85 million, followed by Germany and France, which respectively imposed fines totaling $84 million and $66 million, the law firm says. Post-Brexit, the British government says that under U.K. law, GDPR compliance - together with the country's Data Protection Act 2018 - will continue to be enforced, although it says there will be "technical amendments" added "to ensure it can function in U.K. law." In addition, "the Information Commissioner remains the U.K.'s independent supervisory authority on data protection."

Read More on BankInfoSecurity

More #News

- Fueled by Profits, Ransomware Persists in New Year
- Google Chrome now checks for weak passwords, helps fix them

- DDoS-Guard To Forfeit Internet Space Occupied by Parler
- The dynamic duo: How to build a red and blue team to strengthen your cybersecurity
- Hacker blunder leaves stolen passwords exposed via Google search
- Here's How SolarWinds Hackers Stayed Undetected for Long Enough
- NSA urges system administrators to replace obsolete TLS protocols
- FireEye Releases New Open Source Tool in Response to SolarWinds Hack
- Researchers Discover Raindrop — 4th Malware Linked to the SolarWinds Attack
- DNSpooq lets attackers poison DNS cache records
- GDPR: German laptop retailer fined €10.4m for video-monitoring employees
- Privacy-focused search engine DuckDuckGo grew by 62% in 2020
- Stolen credit card shop Joker's Stash closes after making a fortune
- WhatsApp Delays Controversial 'Data-Sharing' Privacy Policy Update By 3 Months
- How to check if someone else accessed your Google account
- Hackers leaked altered Pfizer data to sabotage trust in vaccines
- Windows Remote Desktop servers now used to amplify DDoS attacks
- Microsoft Edge gets a password generator, leaked credentials monitor

#Breach Log

- Hacker leaks full database of 77 million Nitro PDF user records
- Hacker posts 1.9 million Pixlr user records for free on forum
- OpenWRT Project Community Investigating Data Breach

#Patch Time!

- Microsoft warns of incoming Windows Zerologon patch enforcement
- Multiple backdoors and vulnerabilities discovered in FiberHome routers
- Chrome 88 Drops Flash, Patches Critical Vulnerability
- Cisco Patches Critical Vulnerabilities in SD-WAN, DNA Center, SSMS Products
- Drupal Updates Patch Another Vulnerability Related to Archive Files
- Oracle's January 2021 CPU Contains 329 New Security Patches
- Tens of Vulnerabilities in Siemens PLM Products Allow Code Execution
- Undisclosed Apache Velocity XSS vulnerability impacts GOV sites

#Tech and #Tools

- Snort 3 officially released
- KindleDrip — From Your Kindle's Email Address to Using Your Credit Card
- Kids find a security flaw in Linux Mint by mashing keys
- Falco vs. AuditD from the HIDS perspective
- Bad Pods: Kubernetes Pod Privilege Escalation
- Using Zero Trust principles to protect against sophisticated attacks like Solorigate
- Test a TLS server
- LazyWeb - Vulnerable Web Application
- Evolving Container Security With Linux User Namespaces
- Prelude Operator: autonomous red team C2 platform

- Prelude Operator: autonomous red team C2 platform
- A day-in-the-life of a purple teamer using Prelude Operator
- How to mitigate Pass-the-Cookie
- Cache poisoning in popular open source packages
- SSL/TLS and PKI History
- Overview for Red Team deployable infrastructure
- MSSQL Lateral Movement
- Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop
- Sailing Past Security Measures In AD
- Using ATT&CK to Score Red Team Engagements

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