Security Newsletter

13 November 2017

Subscribe to this newsletter

"Eavesdropper" Vulnerability Exposes Millions of Private Conversations because of hardcoded secrets

Security researchers have discovered that tens of developers have left API credentials in hundreds of applications built around the Twilio service. Attackers can extract these credentials from the source code of vulnerable apps and gain access to conversations and SMS messages sent by that app — and its users — via Twilio, a cloud platform that allows third-party apps to make and receive phone calls and SMS messages via programmatic APIs to various telephony providers.

"We found the Eavesdropper vulnerability on over 685 enterprise apps (44% Android, 56% iOS) associated with 85 Twilio developer accounts," the Appthority team said in a report published today. Appthority says that around a third of all affected apps are enterprise related, potentially granting attackers access to highly precious financial and business phone calls and SMS alerts.

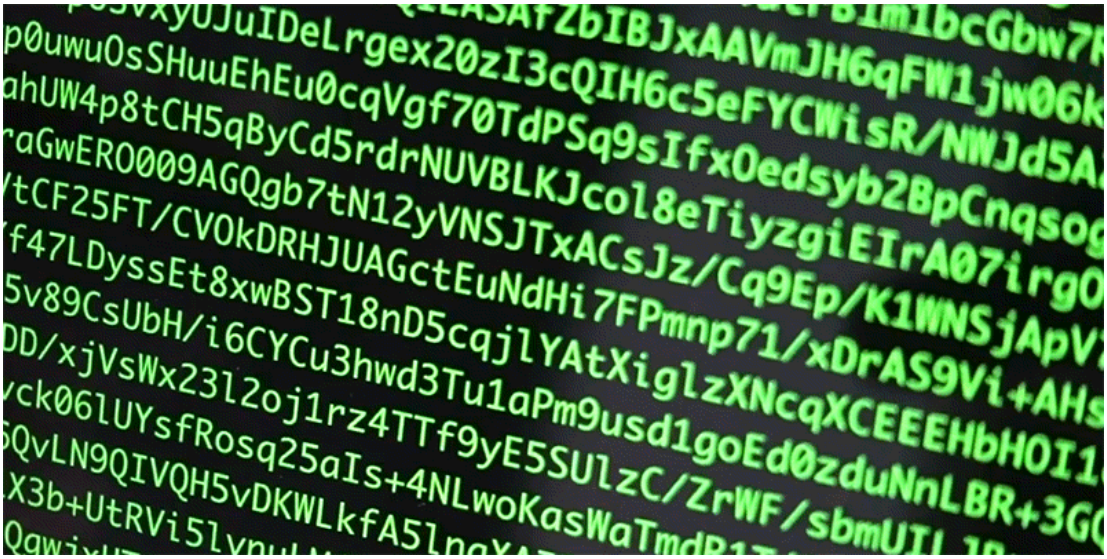
The cause of the Eavesdropper issue is careless developers. We've seen many cases in the past where developers leave API and server credentials inside an app's source code, instead of storing them in a secure, remote database. The same Appthority report on the Eavesdropper vulnerability also points out that researchers found similar credentials for Amazon S3 servers. A Fallible study published earlier this year found that 2,500 of 16,000 Android apps had some type of credentials inside them, usually for services like Twitter, Dropbox, Instagram, Slack, Flickr, or Amazon Web Services (AWS).

If you commit sensitive data, such as a password or SSH key into a Git repository, you can remove it from the history. To entirely remove unwanted files from a repository's history you can use either the git filter-branch command or the BFG Repo-Cleaner. However, be warned: Once you have pushed a commit to GitHub, you should consider any data it contains to be compromised. If you committed a password, change it! If you committed a key, generate a new one.

Read More

Removing sensitive data from a repository

One of the Secrets Guarding the Secure Internet Is a Wall of Lava Lamps



Cloudflare provides security and domain name services for millions of the most prominent sites on the web. The company has built a solid reputation for its secure encryption and one of the key factors in its system is a wall of 100 lava lamps in the lobby of its San Francisco headquarters.

Cryptography relies on the ability to generate random numbers that are both unpredictable and kept secret from any adversary. Unfortunately for cryptographers, if there's one thing computers are good at, it's being predictable. They can execute the same code a million times, and so long as they are given the same inputs each time, they'll always come up with the same outputs. This is very good for reliability, but it's tricky when it comes to cryptography - after all, we need unpredictability!

The solution to this problem is cryptographically-secure pseudorandom number generators (CSPRNGs). But even though CSPRNGs are a very powerful tool, they're only one half of the equation - they still need an unpredictable input to operate. But where can a computer get such unpredictable input, even slowly? The answer is the real world.

A lava lamp is a great way to generate randomness. LavaRand is a system that uses lava lamps as a secondary source of randomness for Cloudflare's production servers. A wall of lava lamps in the lobby of Cloudflare's San Francisco office provides an unpredictable input to a camera aimed at the wall. A video feed from the camera is fed into a CSPRNG.

Hopefully they'll never need it. Hopefully, the primary sources of randomness used by their production servers will remain secure, and LavaRand will serve little purpose beyond adding some flair to their office. But if it turns out that they're wrong, then LavaRand will be the hedge, making it just a little bit harder to hack Cloudflare.

Read More

Randomness 101: LavaRand in Production

60% of developers lack confidence in their app security, but don't take steps to fix it

NodeSource and Sqreen released a study that should be a wakeup call for developers: The majority of them report not trusting the security of their own code. Some 60% of Node.js developers, in fact, say that they aren't confident in the security of the code they write, while only 31% say they are.

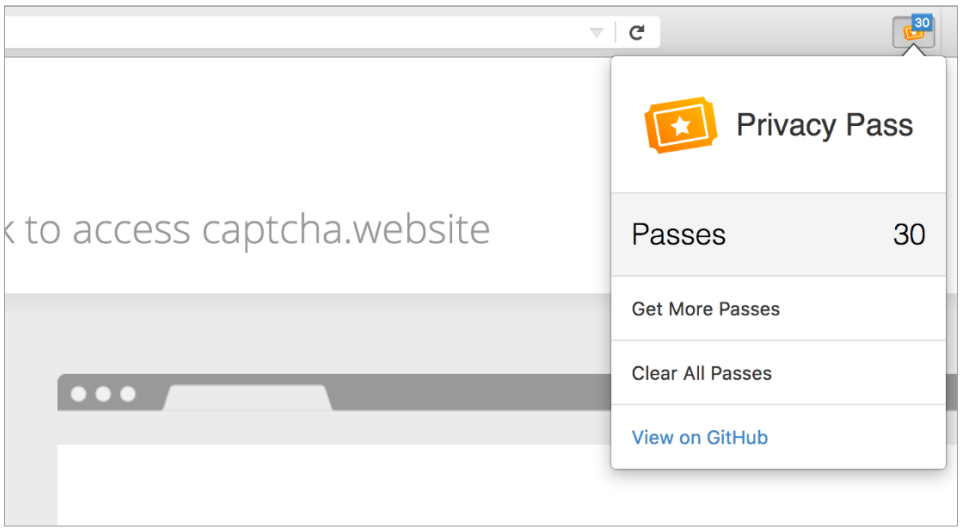
Let's not sell developers short—most of them do review their code in some way, according to the report. Many (44%) perform manual reviews, and 30% perform both manual and automated reviews. Only 12% are guilty of not reviewing their code at all.

Where the real problem comes from, at least in the eyes of the devs doing the coding, is third-party dependencies. Only 16% have confidence in the security of the third-party packages they use. That said, it would make sense for much of the code review process to focus more on outside code. It doesn't, though: 40% said they skip the review process for third-party packages.

Read More

Original study

Privacy Pass: A browser extension for anonymous authentication



There is a new browser extension for Chrome and Firefox named Privacy Pass. Privacy Pass uses privacy-preserving cryptography to allow users to authenticate to services without compromising their anonymity.

Using the extension, users can retrieve 'passes' from services by completing a task of the server's choosing. However, when the user comes to redeem a pass in the future, it will be cryptographically unlinkable from the pass that was received before; even for the service that issued it.

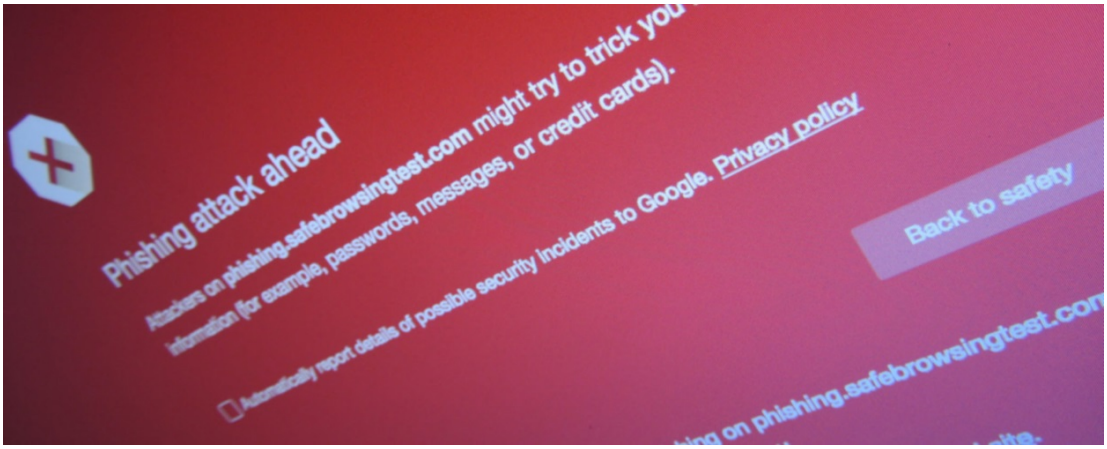
The internet security and performance company Cloudflare is the first partner to implement support for Privacy Pass. Using Privacy Pass with Cloudflare websites allows users to acquire signed 30 tokens for each Cloudflare challenge CAPTCHA that they solve. Once tokens are acquired, users are able to bypass future Cloudflare CAPTCHAs using the redemption phase of the protocol above.

Privacy Pass is released as beta currently, but they hope that releasing it now will encourage more users to get involved in the development process.

Read More

Cloudflare supports Privacy Pass

Google Ranks Phishing Above Keyloggers and Password Reuse as Bigger Threat to Users



Research carried out by Google engineers and academics from the University of California, Berkeley and the International Computer Science Institute has revealed that phishing attacks pose a more significant threat to users losing access to their Google accounts when compared to keyloggers or password reuse.

The research team says it found over 788,000 credentials stolen via keyloggers, 12.4 million credentials stolen via phishing, and 1.9 billion credentials exposed by third-party breaches. "We find victims of phishing are 400x more likely to be successfully hijacked compared to a random Google user. In comparison, this rate falls to 10x for data breach victims and roughly 40x for keylogger victims," the research team added.

In addition, researchers also spotted a rising trend in keyloggers and phishing kits, which are now logging IP addresses and other geolocation data in an attempt to fool geo-based protection filters, while other more complex attack kits also log phone numbers and user-agent string data.

Read More

WikiLeaks' Vault 8 Leaks Show CIA Impersonated Kaspersky Lab

Wikileaks released the source code for Hive on Thursday, a CIA (Central Intelligence Agency) implants used in transferring exfiltrated information from target Windows machines. The latest release has been carried out under the code name of Vault 8. The Vault 8 series will only expose source codes for previously leaked implants.

Hive works as a communication tool between malware and "cover domains." These domains seem harmless and "perfectly-boring-looking" to visitors however traffic from implants communicating with these domains is sent to an implant operator management gateway called Honeycomb. According to WikiLeaks, CIA used these fake certificates to impersonate existing entities including Kaspersky Lab.

In October this year, it was reported that in 2015 Israeli spies managed to access Kaspersky's backend systems and identified that Russian hackers were discreetly using the software both as a universal search engine and a spying tool.

Read More

Flaw crippling millions of crypto keys is worse than first disclosed

A crippling flaw affecting millions—and possibly hundreds of millions—of encryption keys used in some of the highest-stakes security settings is considerably easier to exploit than originally reported, cryptographers declared over the weekend. The assessment came as Estonia abruptly suspended 760,000 national ID cards used for voting, filing taxes, and encrypting sensitive documents.

One way to improve the attack, may be to use fast graphics cards, which have the potential to shave the average cost of factorizing a vulnerable 2048-bit key to $2,000 in energy costs.

Estonia is almost certainly not the only country with a national ID card that's vulnerable to ROCA. Researchers said cards issued by Slovakia also tested positive for the vulnerability. Ars is also aware of unconfirmed reports of a Western European country that also issues affected ID cards.

Read More

Reconstructing ROCA

Cutting room floor

- Find Security Bugs: plugin for security audits of Java web applications
- Antivirus Engine Design Flaw Helps Malware gain boot persistence
- IETF draft to fix SSL spy boxes
- Stack Ranking SSL Vulnerabilities: DUHK and ROCA
- A Guide to Attacking Domain Trusts
- Misconfigured Amazon S3 Expose Companies to MitM Attacks
- Windows Code Injection Technique: PROPagate
- Flaw in Tor Browser Leads to Leaking of Your Real IP Address
- Dnstwist: Find Phishing Sites Based on Your Domain
- Exploring 6 Remote Kernel Bugs on Android Phones
- Google Chrome will automatically block forced website redirects
- Creating Secure Password Resets With JSON Web Tokens
- Evil pixels: Researcher demos data-theft over screen-share protocols
- Credential-stuffing defense tech aims to defuse password leaks
- Default Password list: If you use one of those, change it ASAP!