kindred

Security Newsletter

8 April 2019

Subscribe to this newsletter

540 Million Facebook User Records Found On Unprotected Amazon Servers because of a third party

More than half a billion records of millions of Facebook users have been found exposed on unprotected Amazon cloud servers. The exposed datasets do not directly come from Facebook; instead, they were collected and unsecurely stored online by third-party Facebook app developers.

Researchers at the cybersecurity firm UpGuard today revealed that they discovered two datasets—one from a Mexican media company called Cultura Colectiva and another from a Facebook-integrated app called "At the pool"—both left publicly accessible on the Internet.

More than 146 GB of data collected by Cultura Colectiva contains over 540 million Facebook user records, including comments, likes, reactions, account names, Facebook user IDs, and more. The second dataset belonging to "At the Pool" app contains information about users' friends, likes, groups, and checked-in locations, as well as "names, plaintext passwords and email addresses for 22,000 people."

Read More on TheHackerNews

Even More on SecurityWeek

New Apache Web Server Bug Threatens Security of Shared Web Hosts

Mark J Cox, one of the founding members of the Apache Software Foundation and the OpenSSL project, today posted a tweet warning users about a recently discovered important flaw in Apache HTTP Server software. The Apache web server is one of the most popular, widely used open-source web servers in the world that powers almost 40 percent of the whole Internet.

The flaw affects Apache HTTP Server versions 2.4.17 through 2.4.38 and could allow any less-privileged user to execute arbitrary code with root privileges on the targeted server. According to Cox, the vulnerability is more concerning for shared web hosting services, where malicious customers or a hacker with ability to execute PHP or CGI scripts on a website can make use of the flaw to gain root access on the server, eventually compromising all other websites hosted on the same server.

The vulnerability, identified as CVE-2019-0211, was discovered by Charles Fol, a security engineer at Ambionics Security firm, and patched by the Apache developers in the latest version 2.4.39 of its software released today.

Read More on TheHackerNews

Even More

More #News

- Facebook Demanded User Email Passwords
- Security Strategies for Microservices-based Application Systems: Draft NIST SP 800-204 Available for Comment
- Unpatched Flaw in Xiaomi's Built-in Browser App Lets Hackers Spoof URLs
- GitLab now automatically warns against merging API keys into your codebase
- Financial Mobile Apps Fail to Follow Proper Security Standards
- Introducing Warp: Fixing Mobile Internet Performance and Security
- Thousands of Unprotected Kibana Instances Exposing Elasticsearch Databases
- Azure AD Password Protection Available, Lowers Spray Attack Risks
- WordPress iOS app leaked authentication tokens
- In-Depth Analysis of JS Sniffers Uncovers New Families of Credit Card-Skimming Code
- Hackers Could Turn Pre-Installed Antivirus App on Xiaomi Phones Into Malware
- Samsung Galaxy S10 Fingerprint Scanner Tricked with 3D Print
- Digital Privacy at the U.S. Border: Protecting the Data On Your Devices
- Laptop Security while Crossing Borders
- Hacker group has been hijacking DNS traffic on D-Link routers for three months

#Patch Time!

- Patch Android now! April updates fixes three critical flaws
- Apache HTTP Server 2.4 vulnerabilities
- Microsoft Not Concerned About Disclosed Edge, IE Flaws
- Researcher publishes Google Chrome exploit not yet patched in Stable
- Backdoor code found in popular Bootstrap-Sass Ruby library

#Tech and #Tools

- Ghidra source code officially released
- Huawei and Security Analysis
- DetectionLab: lab environment complete with security tooling and logging best practices
- Using a Yubikey as smartcard for SSH public key authentication
- Go Phishing (and Reporting)
- Handlebars template injection and RCE in a Shopify app
- How to run AWS CloudHSM workloads on Docker containers
- Active Directory Visualization for Blue Teams and Threat Hunters
- Analysis of a VB Script Heap Overflow (CVE-2019-0666)
- CARPE (DIEM): CVE-2019-0211 Apache Root Privilege Escalation
- fireprox: on the fly HTTP pass-through proxies for unique IP rotation

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