kindred

Security Newsletter

22 October 2018

Subscribe to this newsletter

Zero-day in popular jQuery plugin actively exploited for at least three years

For at least three years, hackers have abused a zero-day in one of the most popular jQuery plugins to plant web shells and take over vulnerable web servers. The vulnerability impacts the jQuery File Upload plugin, which is the second most starred jQuery project on GitHub, after the jQuery framework itself. It is immensely popular and has been integrated into many other projects, such as CMSs, CRMs, Intranet solutions, WordPress plugins, Drupal add-ons, Joomla components, and so on.

The Akamai researcher says that attackers can abuse this vulnerability to upload malicious files on servers, such as backdoors and web shells. The vulnerability has been exploited in the wild. "I've seen stuff as far back as 2016". The developer's investigation identified the true source of the vulnerability not in the plugin's code, but in a change made in the Apache Web Server project dating back to 2010, which indirectly affected the plugin's expected behavior on Apache servers.

Blueimp's jQuery File Upload plugin was coded to rely on a custom .htaccess file to impose security restrictions to its upload folder, without knowing that five days before, the Apache HTTPD team made a breaking change that undermined the plugin's basic design. Identifying all affected projects and stomping out this vulnerability will take years.

Read More on ZDNet

Even More on DarkReading

Facebok: Update on security issues: 30M accounts leaked

Facebook has just announced additional details on last month's data breach. The company now says that only 30 million accounts had their access tokens stolen instead of the 50 million they had originally believed, and of those 30 million, 15 million users just had their emails and phone numbers taken.

Worse, however, is that for 14 million unlucky users, the hackers were able to access both email info and phone numbers plus their "username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches" as well.

In an updated post on Facebook's newsroom, the company says it's working with the FBI, who is actively investigating the situation, and therefore can't reveal who they believe were behind the attack. People can check whether they were affected by visiting Facebook Help Center. In the coming days, they will send customized messages to the 30 million people affected to explain what information the attackers might have accessed, as well as steps they can take to help protect themselves, including from suspicious emails, text messages, or calls.

Official Facebook advisory

Even More on TechRadar

Try the hack for yourself on Adversary!

Hacker: I'm logged in. New LibSSH Vulnerability: OK! I believe you.

Newly released versions of the libssh library fix an authentication bypass flaw that grants access to the server by just telling it that the procedure was a success.

The libssh library enables support of the Secure Shell (SSH) protocol in applications, allowing an encrypted connection between clients and servers. Leveraging it is a simple matter of presenting the server with the SSH2_MSG_USERAUTH_SUCCESS message, which shows that the login already occurred without a problem. The server expects the message SSH2_MSG_USERAUTH_REQUEST to start the authentication procedure, but by skipping it an attacker can log in without showing any credentials.

The trick is possible in library versions 0.6 and above, and there is no workaround available, informs an advisory on Thursday from the libssh team. The issue has been addressed in revisions 0.8.4 and 0.7.6 of the library.

Read More on BleepingComputer

Even More

More #News

- NIST Preparing a Privacy Framework
- 35 Million U.S Voter Records Selling in Popular Dark web Hacking Forum from $150 USD to $12,500 USD
- MIT invention builds memory walls to protect against Meltdown, Spectre attacks
- Pentagon Data Breach Exposes up to 30,000 Travel Records
- GreyEnergy: Updated arsenal of one of the most dangerous threat actors
- IE, Edge, Safari, Firefox, Chrome, all planning to deprecate TLS 1.0. 1.1 by 2020
- New iPhone Passcode Bypass Method Found Days After Patch
- Google to Encrypt Android Cloud Backups With Your Lock Screen Password
- Supply Chain Security 101: An Expert's View
- DOM-based XSS Vulnerability Affected 685 Million Users of Tinder, Shopify, Western Union, and Imgur
- Decoding the Google Titan, Titan, and Titan M – that last one is the Pixel 3's security chip
- Apple's New Data & Privacy Portal Lets You Download Your Data
- Tumblr Fixes Security Bug that Leaked Private Account Info
- Novel user tracking technique involving HTTPS (TLS) session resumption.

#Patch Time!

- Oracle patches 301 vulnerabilities, including 46 with a 9.8+ severity rating
- LibSSH Advisory
- Cisco Security Advisories: 7 High vulns
- Windows 10 Cumulative and Compatibility Updates Released
- Splunk Patches Several Flaws in Enterprise, Light Products

#Tech and #Tools

- Persistent Credential Theft with Authorization Plugins
- Browsing Experience Security Check
- Detecting Encrypted Malware Traffic (Without Decryption)
- Four Ways to Bypass iOS SSL Verification and Certificate Pinning
- Route 53 as Pentest Infrastructure
- Forging Trusts for Deception in Active Directory
- GrayHatWarfare Bucket search updated
- Deobfuscating PowerShell: Putting The Toothpaste Back In The Tube
- Excel for Infosec #BestSIEMEver
- Which Base Image should you use for your containers?
- MemITM: Tool to make in memory man in the middle
- Curious how Facebook got hacked? Try it for yourself!

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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