kindred

Security Newsletter

11 September 2017

Subscribe to this newsletter

Critical Apache Struts vulnerability under “massive” attack

Apache Struts 2 installations have been targeted - and hacked in large numbers - by attackers who were exploiting a (now patchable) zero-day flaw in the platform to remotely execute code, security researchers warn.

Open source Apache Struts 2 is a widely used computing platform that runs Java Enterprise Edition. Numerous sites use Struts, including airlines, car-rental firms and e-commerce shops as well as not-for-profit organizations, social networks and government agencies.

The remote-code execution vulnerability in Struts that's being actively exploited - CVE-2017-5638 - exists in the Jakarta Multipart parser, which is used for uploading files. An attacker can exploit the flaw for unauthenticated remote code execution by crafting a special Content-Type value in an HTTP request.

Researchers at Cisco Systems said they are seeing a "high number of exploitation events" by hackers attempting to carry out a variety of malicious acts. One series of commands that attackers are injecting into webpages stops the firewall protecting the server and then downloads and executes malware of the attacker's choice. The payloads include "IRC bouncers," which allow the attackers to hide their real IP address during Internet chats; denial-of-service bots; and various other packages that conscript a server into a botnet.

Apache Struts versions affected by the vulnerability include Struts 2.3.5 through 2.3.31, and 2.5 through 2.5.10. Servers running any of these versions should upgrade to 2.3.32 or 2.5.10.1 immediately. While most bug fixes require downloading and installing a patch, possibly rebooting a machine, and being done with it. The fix here, by contrast, typically requires each Web app that was developed with a vulnerable version of Apache Struts to be recompiled using a patched version.

Read More

Patch note

Breach at Equifax May Impact 143M Americans

Equifax, one of the “big-three” U.S. credit bureaus, said today a data breach at the company may have affected 143 million Americans, jeopardizing consumer Social Security numbers, birth dates, addresses and some driver’s license numbers.

Equifax said the investigation is still ongoing, but that the breach also jeopardized credit card numbers for roughly 209,000 U.S. consumers and “certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers.”

The attackers were able to break into the company’s systems by exploiting an application vulnerability to gain access to certain files. Equifax did not say which application or which vulnerability was the source of the breach. Bloomberg reports that three Equifax senior executives sold shares worth almost $1.8m in the days after the company discovered the breach – but before Thursday’s disclosure.

Read More

Even More

There's no such thing as too small to hack

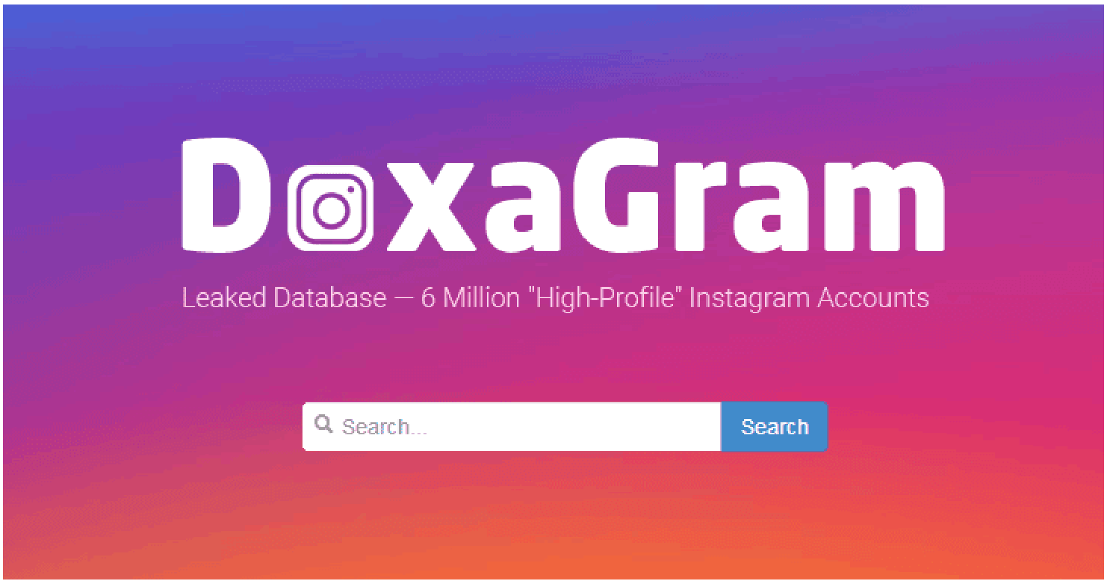
Small business owners all-too-frequently believe that they won't be targeted by hackers because they don't offer anything of interest to cybercriminals. Since mainstream media outlets tend to solely focus on the "spectacular" large corporate and government breaches, it's somewhat understand that this misconception continues to fester. But that narrative may be starting to shift.

The U.S. Securities & Exchange Commission recently stated that SMBs are "at even greater risk, and are far more vulnerable once they are victimized." As the volume of attacks and lucrative profits continue to grow, all business owners – from Fortune 100 companies to small family-owned businesses – need to get serious about defending their business websites from being compromised.

Small businesses that are hacked often suffer losses of much greater magnitude than their larger counterparts because they lack the established "name recognition" of big companies. Hackers may use a site to host malware, to get around blacklisted IP addresses, which can gravely affect company's marketing efforts by hurting their search engine rankings on Google, Bing and many others. If a company's site is detected as compromised, search engines will devalue a domain until its able to rid it of malicious code.

Read More

6 Million Instagram Accounts Hacked: How to Protect Yourself



Leaked Database — 6 Million "High-Profile" Instagram Accounts

Several days ago, Instagram announced that it had fixed a vulnerability that had apparently previously allowed unauthorized parties to obtain the email addresses and phone numbers associated with Instagram accounts, even when such information was supposed to be private and inaccessible to parties other than respective account owners.

Armed with the pilfered information, criminals could potentially have attempted to trigger and intercept password reset messages or to phish or otherwise social engineer Instagram users -- which may explain how Gomez's account was breached. Before the bug was fixed by Instagram, a hacker, or group of hackers, apparently stole a significant amount of data that he/she/they are now offering for sale online at a price of $10 per record on a platform called "Doxagram".

The party responsible for Doxagram says that it amassed data from over six million users. Of course, Instagram has over 700 million active monthly users, so six million is fewer than 1 percent of the total Instagram userbase -- but, it still represents many potentially unhappy people.

Read More

More on Doxagram

Lenovo settles lawsuits with 32 states over the spyware scandal Superfish

From August 2014 to December 2014, Lenovo sold laptops that had Visual Discovery spyware pre-installed, as Naked Security's Paul Ducklin discussed back in February 2015. Visual Discovery is software that's developed by Superfish, which describes itself as a marketing company.

Visual Discovery compares images you see in your web browser to its massive cloud database of images. If a Lenovo customer agreed to have Visual Discovery installed on their laptop for whatever reason, there would have been less of an ethical problem. But a lot of people who bought Lenovo laptops in the last quarter of 2014 were unaware that what amounted to spyware was pre-installed on their Windows OEM PCs. Even worse, to get the information whatever browser you used, Visual Discovery performed as a man in the middle for all HTTPS connections.

Fast forward to now, September 2017, and Lenovo has settled a lawsuit from the US's Federal Trade Commission, the state of Connecticut, and 31 other American states, for $3.5m. According to a decision published on the FTC's website, the Chinese hardware vendor has dodged crippling financial penalties. Instead, the FTC has "prohibited" Lenovo from "misrepresenting any features" in case it will ever decide to install adware on users' laptops. Many thinks the entire punishment is a joke taking into consideration what it's about. An FTC complaint was filed soon after. Yesterday's settlement is only a proposal. The FTC will listen for public comment for 30 days before making it final or adjusting the punishment.

Read More

Even More

Yet another AWS config fumble: Time Warner Cable exposes 4 million subscriber records

Records of roughly four million Time Warner Cable customers in the US were exposed to the public internet after a contractor failed to properly secure an Amazon cloud database. Researchers said freelancers who handled web applications for TWC and other companies had left one of its AWS S3 storage bins containing seven years' worth of subscriber data wide open on the 'net. That data included addresses and contact numbers, information about their home gateways, and account settings.

The researchers found that the database included information on four million TWC customers collected between November 26, 2010 and July 7, 2017. The exposed data included customer billing addresses, phone numbers, usernames, MAC addresses, modem hardware serial numbers, account numbers, and details about the service settings and options for the accounts.

Unfortunately, oftentimes developers like to simplify their life or quickly resolve some technical problems and grant public read access to the buckets There are at least two tools already provided by AWS to detect this critical security flaw with your S3 buckets - AWS Trusted Advisor and AWS Config.

Read More

Even More

Software to capture votes in upcoming Germany's national election is insecure

The Chaos Computer Club is publishing an analysis of software used for tabulating the German parliamentary elections (Bundestagswahl). The analysis shows a host of problems and security holes, to an extent where public trust in the correct tabulation of votes is at stake. Proof-of-concept attack tools against this software are published with source code.

According to the CCC analysis, vulnerabilities could lead to multiple practicable attack scenarios that eventually allow malicious agents in the electoral office to change total vote counts.

The hacker collective found that the automatic software update module of PC-Wahl downloads packages over insecure HTTP connection and does not perform any integrity check using digital signatures. Moreover, the software uses an older encryption method with a single secret key hard-coded in the software, rather than asymmetrical encryption that offers better security by design.

Election hacking has become a major debate following the 2016 US presidential election, where it was reported that Russian hackers managed to access United States voting machines in 39 states in the run-up to the election. However, there is no evidence yet to justify the claims.

Read More

Original statement from CCC

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