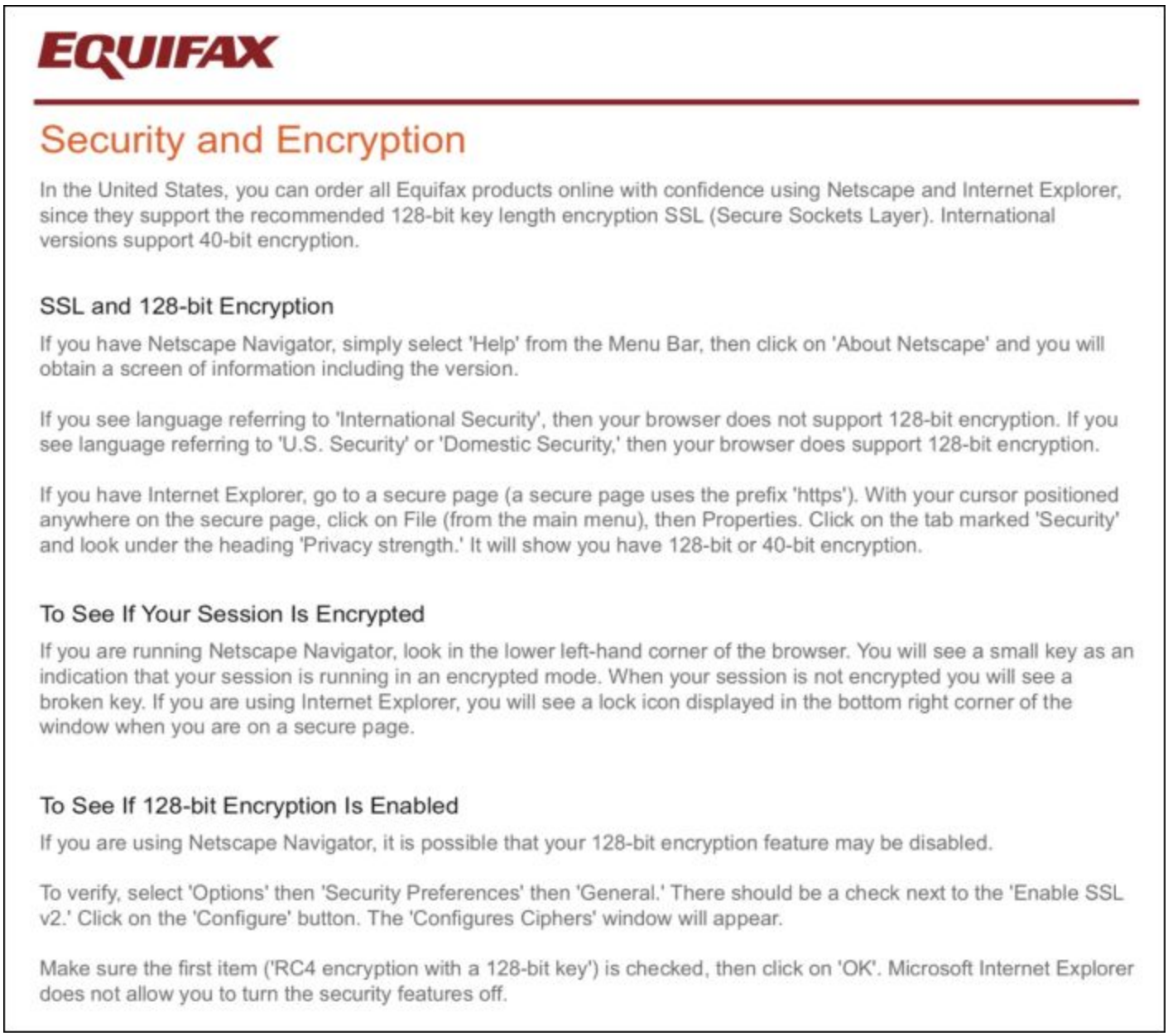
Security Now! #628 - 09-12-17

The Equifax Fiasco

This week on Security Now!

This week we discuss last Friday's passing of our dear friend and colleague Jerry Pournelle, when AI is turned to evil purpose, whether and when Google's Chrome browser will warn of man in the middle attacks, why Google is apparently attempting to patent pieces of a compression technology they did not invent, another horrifying router vulnerability disclosure -- including ten 0-day vulnerabilities, an update on the sunsetting of Symantec's CA business unit, another worrying failure at Comodo, a few quick bits, an update on my one commercial product SpinRite, answering a closing the loop question from a listener, and a look at the Equifax fiasco.

Our *(Distressing)* Picture of the Week



EQUIFAX

Security and Encryption

In the United States, you can order all Equifax products online with confidence using Netscape and Internet Explorer, since they support the recommended 128-bit key length encryption SSL (Secure Sockets Layer). International versions support 40-bit encryption.

SSL and 128-bit Encryption

If you have Netscape Navigator, simply select 'Help' from the Menu Bar, then click on 'About Netscape' and you will obtain a screen of information including the version.

If you see language referring to 'International Security', then your browser does not support 128-bit encryption. If you see language referring to 'U.S. Security' or 'Domestic Security,' then your browser does support 128-bit encryption.

If you have Internet Explorer, go to a secure page (a secure page uses the prefix 'https'). With your cursor positioned anywhere on the secure page, click on File (from the main menu), then Properties. Click on the tab marked 'Security' and look under the heading 'Privacy strength.' It will show you have 128-bit or 40-bit encryption.

To See If Your Session Is Encrypted

If you are running Netscape Navigator, look in the lower left-hand corner of the browser. You will see a small key as an indication that your session is running in an encrypted mode. When your session is not encrypted you will see a broken key. If you are using Internet Explorer, you will see a lock icon displayed in the bottom right corner of the window when you are on a secure page.

To See If 128-bit Encryption Is Enabled

If you are using Netscape Navigator, it is possible that your 128-bit encryption feature may be disabled.

To verify, select 'Options' then 'Security Preferences' then 'General.' There should be a check next to the 'Enable SSL v2.' Click on the 'Configure' button. The 'Configures Ciphers' window will appear.

Make sure the first item ('RC4 encryption with a 128-bit key') is checked, then click on 'OK'. Microsoft Internet Explorer does not allow you to turn the security features off.

Security News

Last Friday Jerry Pournelle passed away quietly in his sleep.

- His son, Alex, wrote:
  I'm afraid that Jerry passed away. We had a great time at DragonCon. He did not suffer.

- Born August 7th, 1933 in Shreveport, Louisiana

- Celebrated his 84th birthday a month ago on August 7

- Roberta is a big hugger and it always seemed to mildly annoy him that she and I would always give each other an overly long embrace whenever we the three of us bumped into each other, which happened quite a bit back in the early days of the PC and pre-PC industry. Jerry would just stand there, with his string tie, looking annoyed and waiting for us to be done.

- IMO, "The Mote in God's Eye", Co-written with Larry Niven, was their master work.

- https://www.jerrypournelle.com/chaosmanor/

AI is already being explored to increase phishing and hacking efficiency
https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425
Title: "Hackers Have Already Started to Weaponize Artificial Intelligence"

Last year, two data scientists from security firm ZeroFOX conducted an experiment to see who was better at getting Twitter users to click on malicious links, humans or an artificial intelligence. The researchers taught an AI to study the behavior of social network users, and then design and implement its own phishing bait. In tests, the artificial hacker was substantially better than its human competitors, composing and distributing more phishing tweets than humans, and with a substantially better conversion rate.

The AI, named SNAP_R, sent simulated spear-phishing tweets to over 800 users at a rate of 6.75 tweets per minute, luring 275 victims. By contrast, Forbes staff writer Thomas Fox-Brewster, who participated in the experiment, was only able to pump out 1.075 tweets a minute, making just 129 attempts and luring in just 49 users.

Thankfully this was just an experiment, but the exercise showed that hackers are already in a position to use AI for their nefarious ends. And in fact, they're probably already using it, though it's hard to prove. In July, at Black Hat USA 2017, hundreds of leading cybersecurity experts gathered in Las Vegas to discuss this issue and other looming threats posed by emerging technologies. In a Cylance poll held during the confab, attendees were asked if criminal hackers will use AI for offensive purposes in the coming year, to which 62 percent answered in the affirmative.

I did the math, the "capture" or "conversion rate" was nearly the same for both human and AI. 34.4% vs 38.0% which is not a statistically significant difference for such small sample sizes. So that's about the same.

The advantage the AI did have was typing speed.

Google Chrome Will Soon Warn You of [some poor] Software That Performs MitM Attacks
https://www.bleepingcomputer.com/news/security/google-chrome-will-soon-warn-you-of-software-that-performs-mitm-attacks/

> Google Chrome 63 will include a new security feature that will detect when third-party software is performing a Man-in-the-Middle (MitM) attack that hijacks the user's Internet connection.
>
> For the party performing the MitM attack, the hardest part is dealing with encrypted HTTPS traffic. Most MitM toolkits fail to correctly rewrite the user's encrypted connections, causing SSL errors that Chrome will detect.
>
> Chrome will show an error when it suspects MitM attacks
>
> The new Chrome 63 feature is in the form of a new warning screen. This new error will appear whenever Chrome detects a large number of SSL connection errors in a short timespan, a sign that someone is trying — and failing — to intercept the user's web traffic.
>
> This includes both malware and legitimate applications, such as antivirus and firewall applications. The new Chrome error won't show up for all antivirus and firewall software, but only for those that do not rewrite SSL connections in a proper way, resulting in SSL errors.

So THAT's an important distinction -- only WRONGLY intercepted MITM.

What about Google Chrome's own certificate pinning? Are MITM middleboxes deliberately passing Google-ended connections? We KNOW that many fake Google certs have been caught by Chrome... and ANY MITM interception would be presenting a pin-breaking certificate to the browser.

Google Accused of Trying to Patent Public Domain Technology
https://www.bleepingcomputer.com/news/google/google-accused-of-trying-to-patent-public-domain-technology/

A Polish academic (assistant professor Jaroslaw (Jarek) Duda) is accusing Google of trying to patent technology he invented and that he purposely released into the public domain so companies like Google couldn't trap it inside restrictive licenses.

The technology's name is Asymmetric Numeral Systems (ANS), a family of entropy coding methods that Polish assistant professor Jaroslaw (Jarek) Duda developed between 2006 and 2013.

ANS is a game changer for data compression

Over the years, due to its many advantages, variations of Duda's ANS technology — tANS and rANS — have been adopted in several data compression systems, such as Apple's LZFSE compressor, Facebook's Zstandard compressor, and Google's Draco 3D compressor.

Further, ANS is also currently considered for the coding phase of AV1, an upcoming open video coding format.

Tech companies are choosing Duda's ANS technology because it provides faster compression and decompression speeds with minimal data loss, without the downside of a huge computational cost. Rough estimations show that Duda's ANS is between 3 to 30 times faster when compared to classic Huffman and arithmetic coding techniques used in the past.

It is no wonder that whoever holds an ANS-related patent could be in line for some pretty big royalty fees in the upcoming future.

And... Google has filed for an ANS-related patent in over 100 countries

One of the first companies that tried to patent ANS-related technology was StoreLeap in the UK, but Duda moved quickly to block the company's application with the UK Intellectual Property Office, nonetheless, the patent is very close to being approved in the US.

Duda is now in for a bigger fight, as the world's most valuable company — Google — has also filed a similar patent application in the US and more than 100 other countries.

The researcher has not taken Google's patent application lightly, calling it a "nice 'thank you' from a multibillion 'don't be evil' corporation to a poor academic whose work they use for free."

Researcher intentionally released ANS into public domain

In a patent application complaint he filed in the US and with WIPO officials, Duda specifically mentions that he published all ANS research in the public domain to "protect its use from becoming a legal minefield."

Duda also points out that Google was well aware of his work, and he even helped Google's staff implement ANS for video file compression.

The researcher now claims that Google is trying to patent some of the same concepts he shared with the company's engineers.

Duda wrote: "The content of this patent application is a direct natural modification of a textbook way for encoding transform coefficients that represent image blocks in video/image compression. This approach is well known."

He continues: "The concerned patent application also briefly introduces well-known basic techniques of ANS [...], used by dozens of people in various public implementations. While the implementation I have helped them with was for a specific variant of ANS (rANS variant to be exact), this patent application is written in a more general way to restrict free use also of other ANS variants (especially tANS)."

"Despite dubious innovation claims, this application can be seen as a legal risk for both the existing ANS-based image compressors (like GST) and for other parties considering ANS for future image and video compressors. Therefore, I am requesting the rejection of this application," Duda vehemently asked of USPTO and WIPO in his complaint.

Patent orgs may side with Polish researcher

The International Search Authority [ISA], a WIPO department tasked with searching prior patents, has already sided with Duda on the topic and published a scathing review, calling Google's patent as NOT comprising "an inventive contribution over the prior art, because it is no more than a straightforward application of known coding algorithms."

Writing on online forums, Duda said he had high hopes when he first reached out to Google.

"There was a moment they gave me hope for a formal collaboration with my University so I could build a team, but then silence ... probably due to this patent application," the researcher wrote.

"[Right now,] Google is not responding, probably currently rewriting the patent - showing its determination to reach this monopoly," the researcher told Bleeping Computer via email.

The university that employs Duda's, which often touts the researcher's accomplishments, has also pledged public support for the assistant professor's current efforts to defend his invention.

Google did not reply to a request for comment. The article will be updated with any official statement if the company decides to provide context for its patent application.

The mystery remains surrounding Google's decision to patent something that is in the public domain since 2014.

TEN (count'em) DLink Router 0-days publicly disclosed by their discoverer after D-Link refused to cooperate.
https://pierrekim.github.io/blog/2017-09-08-dlink-850l-mydlink-cloud-0days-vulnerabilities.html
https://pierrekim.github.io/blog/2017-02-02-update-dlink-dwr-932b-lte-routers-vulnerabilities.html

The Dlink 850L is a Wireless AC1200 Dual Band Gigabit "Cloud" Router.

Mydlink Cloud Services allow you to access, view and control the devices on your home network from anywhere.

The hacker initially examined the router for participation in a contest and was appalled by what he found. DLink never worked with him, but after months of no apparent action claimed that someone discovered some problems by accident...

Summary of the flaws discovered and published:

Firmware "protection": The latest firmware for version A is not protected and firmware images can be forged by attackers. Version B firmware is password-protected with a hardcoded password -- in other words, extremely poorly.

- WAN & LAN - revA - XSS: PHP files found within the router system can be exploited and if attackers use a number of XSS flaws within, they can steal authentication cookies.

- WAN & LAN - revB - Retrieving admin password, gaining full access using the custom mydlink Cloud protocol: Without breaking D-Link's terms of use, Kim found vulnerabilities which could allow attackers to abuse the MyDLink cloud protocol and register the router to their own accounts to gain full, unfettered access.

- WAN - revA and revB - Weak Cloud protocol: The MyDlink Cloud protocol is little more than a basic TCP relay system and has no encryption by default. Traffic is sent over TCP to Amazon servers without encryption. To make matters worse, the router interface allows users to enter credentials for their email accounts, which are then sent from the router to server without encryption or suitable verification. Passwords are also stored in cleartext.

- LAN - revB - Backdoor access: The router model has a backdoor which can be accessed by logging in with Alphanetworks and a supplied password, granting an attacker root access and control.

- WAN & LAN - revA and revB - Stunnel private keys: The router's stunnel private keys are hardcoded, which paves the way for SSL Man-in-The-Middle (MiTM) attacks.

- WAN & LAN - revA - Nonce bruteforcing for DNS configuration: DNS configuration can be changed without admin user authentication checks, allowing for routing and bruteforce attacks.

- Local - revA and revB - Weak files permission and credentials stored in cleartext: Some files have weak permission setups and store credentials in cleartext.

- WAN - revB - Pre-Auth RCEs as root (L2): The DCHP client running on the router is vulnerable to a number of command injections as root, leading to potential remote code execution. If a vulnerable router is connected to an internal network, the attack will also make the network vulnerable to exploit.

- LAN - revA and revB - DoS against some daemons: A number of daemons can be crashed remotely.

Google Security Blog: Chrome distrusting Symantec Certs
https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
September 11, 2017

This provides a bit of Google-side perspective about the Symantec/DigiCert agreement and what the sunsetting of Symantec-signed certs mean -- practically -- for website operators:

"After our agreed-upon proposal was circulated, Symantec announced the selection of DigiCert to run this independently-operated Managed Partner Infrastructure, as well as their intention to sell their PKI business to DigiCert in lieu of building a new trusted infrastructure.

This post outlines the timeline for that transition and the steps that existing Symantec customers should take to minimize disruption to their users.

Information For Site Operators

Starting with Chrome 66, Chrome will remove trust in Symantec-issued certificates issued prior to June 1, 2016. Chrome 66 is currently scheduled to be released to Chrome Beta users on March 15, 2018 and to Chrome Stable users around April 17, 2018.

If you are a site operator with a certificate issued by a Symantec CA prior to June 1, 2016, then prior to the release of Chrome 66, you will need to replace the existing certificate with a new certificate from any Certificate Authority trusted by Chrome.

Additionally, by December 1, 2017, Symantec will transition issuance and operation of publicly-trusted certificates to DigiCert infrastructure, and certificates issued from the old Symantec infrastructure after this date will not be trusted in Chrome.

Around the week of October 23, 2018, Chrome 70 will be released, which will fully remove trust in Symantec's old infrastructure and all of the certificates it has issued. This will affect any certificate chaining to Symantec roots, except for the small number issued by the independently-operated and audited subordinate CAs previously disclosed to Google.

Site operators that need to obtain certificates from Symantec's existing root and intermediate certificates may do so from the old infrastructure until December 1, 2017, although these certificates will need to be replaced again prior to Chrome 70. Additionally, certificates issued from Symantec's infrastructure will have their validity limited to 13 months. Alternatively, site operators may obtain replacement certificates from any other Certificate Authority currently trusted by Chrome, which are unaffected by this distrust or validity period limit.

Remember that we're are used to client-side OSes which have a massive store of all trusted CA self-signed root certificates which can be used to verify the signatures of server certs.

But, for example, IoT devices from a given manufacturer may be resource constrained and may ONLY be carrying a Symantec root cert... under the previously valid assumption that any certs signed by that root would always be valid and that the servers the IoT device connects with would always be signed with the Symantec root.

CAA checking becomes mandatory on Friday (9/8/2017)

And COMODO, who's site brags about being CAA-compliant, issues a cert in direct contravention of a researcher's CAA record.
https://www.bleepingcomputer.com/news/security/comodo-caught-breaking-new-caa-standard-one-day-after-it-went-into-effect/

www.grc.com. CAA 0 issue "digicert.com"

Comodo has its heart in the right place:
https://support.comodo.com/index.php?/Knowledgebase/Article/View/1204/1/caa-record---certification-authority-authorization

But apparently not its technology. :-/

A security researcher, whose DNS CAA record specified LetsEncrypt as its domain's ONLY authorized server certificate signer... obtained a new certificate from Comodo in direct contravention of the CAB certificate issuance guidelines on September 8th, a day after the enforcement of CAA checking before issuance had become mandatory. (Note that it should have been standard practice already for some time.)

German security researcher Hanno Böck says he obtained the certificate last Saturday, a day after CAA checks became mandatory on Friday, September 8, 2017.

"I was originally informed about the lack of CAA checking at Comodo by Michael Kliewe from the mail provider mail.de," Böck wrote in a mailing list. "However that was before CAA became mandatory."

"I have by now heard from multiple other people that confirmed the same. Seems right now Comodo isn't checking CAA at all."

Quick Bits

VW engineer sent to the clink for three years for emissions-busting code
James Liang gets 40 months on the cooler and $200,000 fine
http://www.theregister.co.uk/2017/08/25/vw_engineer_gets_3yrs_for_emissionbusting_sw/

As head of the VW's Diesel Competence unit in the US, Liang oversaw the software function that enabled the cars to cheat the emissions tests. He is also the most junior of the eight current and former VW executives that have been charged so far.

The "defeat device" was designed to recognize when the car was being tested (effectively noting that the wheels were turning but the car wasn't moving) and switch to a lower emissions setting.

When the car was running normally, that setting was removed and emissions were measured at up to 40 times higher than the permitted levels. The device was fitted on 11 million cars.

The engineers knew full well what they were doing and attempted to hide their tracks, even calling the device a variety of pseudonyms including "acoustic function," "cycle beating software" and "emissions-tight mode."

Federal prosecutor Mark Chutkow said Liang's prison sentence would send "a powerful deterrent message to the rest of the industry."

It's not just the auto industry that will hear the message. Software engineers across the country will have to reflect on the fact that they may be held personally responsible for creating something that knowingly breaks the law (cough, cough, Uber).

iOS 11 to hide Ethernet MAC addresses from Apps
Jeff Wilson: https://twitter.com/jeffwilsontech/status/901852890863566848
This week in Internet Marketers have ruined the internet: iOS11 apps won't be able to access arp table due to abuse by marketers.

SpinRite

- What is SpinRite?
- The v6.x plan
- The v7.0 plan
- The v6.x pre-release plan

Closing The Loop

Ed Zucker (@EdZucker)
@SGgrc What do you think about Tarsnap as a replacement for CrashPlan?

- "Online backups for the truly paranoid" (we would say "for the sufficiently cautious")
- Tarsnap runs on UNIX-like operating systems (BSD, Linux, MacOS X, Cygwin, etc).
- A local hash is maintained of blocks.
- When backing up, the hash blocks are checked for "deduplication."
- Only new data is processed.
- It is first added to the hash.
- Then compressed.
- Then locally encrypted.
- Then uploaded to the Tarsnap cloud servers.
- https://www.tarsnap.com/index.html
- It is Colin's "Scrypt" that I chose as the basis for SQRL's memory-hard acceleration resistant PBKDF.

The Equifax Fiasco

A listener wrote: @SGgrc, not an American so I don't really understand what Equifax does. Mayhaps there'll be an explanation on this week's #securitynow.

Equifax, Experian and TransUnion.

Data sharing: lenders and history aggregators.

"Credit Score"

What happened?

Equifax lost control of their database of highly detailed quietly collected and private consumer credit data for 143 Million US consumers -- 44% of US population.

Information accessed included names, social security numbers, birth dates, addresses, and in some instances driver's license numbers. A smaller number of credit card numbers (209k), dispute documents (182k), and information on UK and Canadian residents also accessed.

Equifax is believed to have first become aware of the incident on July 29, while the breach is believed to have occurred from mid-May through July. So that's half of May, June and July -- or ~2.5 months of unauthorized access to the most sensitive and privacy-requiring consumer financial data before the intrusion was detected. This, of course, raises broad concerns regarding Equifax's overall data security and practices.

And... after learning of the breach, Equifax kept it secret for five weeks... while their database was leaked and the personal details of 143 million US consumers was at risk.

So Equifax was first unaware of the breach for about two and a half months, then they waited for five weeks after learning about it -- while sensitive consumer data was in the wild -- before disclosing this to the public so that the public could take action to protect themselves.

Incidentally... three of Equifax's executives sold $1.8 million of Equifax stock, but there is no evidence that they were aware of the breach.

What do we know about the breach's underlying vulnerability?

Apache Struts - A Server-side JAVA-based web design framework.

It's a sophisticated system that needs to be used responsibly. It's powerful and not highly hand holding. So it requires competent developers. As we'll see in a bit when we talk about the generation of per-user unlock authentication PINs, the competence and attention to detail of Equifax's developers could be easily called into question.

René Gielen Vice President, Apache Struts for the Apache Struts Project Management Committee.

https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax

<quote> The Apache Struts Project Management Committee (PMC) would like to comment on the Equifax security breach, its relation to the Apache Struts Web Framework and associated media coverage.

We are sorry to hear news that Equifax suffered from a security breach and information disclosure incident that was potentially carried out by exploiting a vulnerability in the Apache Struts Web Framework.

At this point in time it is not clear which Struts vulnerability would have been utilized, if any. In an online article published on Quartz.com [1], the assumption was made that the breach could be related to CVE-2017-9805, which was publicly announced [eight days ago] on 2017-09-04 along with new Struts Framework software releases to patch this and other vulnerabilities.

However, the security breach was detected [by Equifax] in July, which means that the attackers either used an earlier announced vulnerability on an unpatched Equifax server, or exploited a vulnerability not known at this point in time -- a Zero-Day-Exploit.

If the breach was caused by exploiting CVE-2017-9805, it would have been a 0-Day exploit at that time. The article also states that the CVE-2017-9805 vulnerability existed for nine years.

[[snip]] Our general advice to businesses and individuals utilizing Apache Struts as well as any other open or closed source supporting library in their software products and services is as follows:

1. Understand which supporting frameworks and libraries are used in your software products and in which versions. Keep track of security announcements affecting this products and versions.

2. Establish a process to quickly roll out a security fix release of your software product once supporting frameworks or libraries needs to be updated for security reasons. Best is to think in terms of hours or a few days, not weeks or months. Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years.

3. Any complex software contains flaws. Don't build your security policy on the assumption that supporting software products are flawless, especially in terms of security vulnerabilities.

4. Establish security layers. It is good software engineering practice to have individually secured layers behind a public-facing presentation layer such as the Apache Struts framework. A breach into the presentation layer should never empower access to significant or even all back-end information resources.

5. Establish monitoring for unusual access patterns to your public Web resources. Nowadays there are a lot of open source and commercial products available to detect such patterns and give alerts. We recommend such monitoring as good operations practice for business critical Web-based services.

Once followed, these recommendations help to prevent breaches such as unfortunately experienced by Equifax.

In the wake of this news, everyone rushing to lock their reporting has been crashing the sites of all three bureaus.

- Security Now! listeners who followed our advice many years ago were already protected.

- SN #495 / February 17, 2015 / "HTTP/2"

- STEVE: Okay. Lastly, and this is - I probably should have done this first, but these other stories were just too interesting, and the industry's been buzzing about them. I created a bit.ly link for this, and it's important: bit.ly/freezecredit, all lowercase. So bit.ly slash F-R-E-E-Z-E-C-R-E-D-I-T. This takes you to a page where the guy explains that a service that is available to anyone for all three major credit bureaus - Equifax, Experian, and TransUnion - allows consumers who are not the victims of identity theft to lock their credit reports. It's not free, but it's not too expensive. The cost varies, depending upon where you are, from $3 to $10. In California it was $10. And because I was curious to do this, although I wasn't worried about this recent Anthem breach, I locked my credit reports. It was $10 for each of them.

- LEO: You may have to pay to thaw it, as well, and this is important.

http://bit.ly/freezecredit
http://clark.com/personal-finance-credit/credit-freeze-and-thaw-guide/

Weak PINs

- Umm @SGgrc... How much entropy is there in the timestamp?
  Would be great to hear the break down in tomorrow's show :)

Uh... None!

Equifax: While we have confidence in the current system, we understand and appreciate that consumers have questions about how PINs are currently generated. We are engaged in a process that will provide consumers a randomly generated PIN. We expect this change to be effective within 24 hours. A consumer has an option, and will continue to have an option, to change an existing PIN. The requested new PIN is sent to the consumer by US Mail to their address of record.

mmddyyhhmm

https://mobile.nytimes.com/2017/09/10/your-money/identity-theft/equifax-breach-credit-freeze.html?referer=

When Helene Muller-Landau first heard the news about the Equifax security breach, she set about freezing her credit files and those of her husband and mother.

Very quickly, however, Ms. Muller-Landau, a Smithsonian research scientist, noticed something strange: The personal identification numbers that Equifax was assigning her family members (to use for eventually lifting the freezes) were awfully similar.

At first, she thought it was a mistake. Maybe it had to do with the fact that she was in Panama, or that her web browsers were acting up. But no: The Equifax PINs are based on the date and time that you set up your freeze.

"The whole point of a 10-digit PIN is that it's supposed to be hard to guess," she said. "And then, they have this totally transparent algorithm for assigning them."

This is among the worst of the facts that have emerged in the wake of the company's announcement on Thursday that thieves may have stolen up to 143 million Social Security numbers, dates of birth, names and addresses from its credit files. Armed with that information, thieves, blackmailers and enemies can make a lot of mischief. A credit freeze can prevent thieves from using your information to open new accounts, since lenders want to see a credit report before doing business with you.

And, of course, we have the expected class-action lawsuit.

The plaintiffs in the lawsuit are Mary McHill and Brook Reinhard. Both reside in Oregon and had their personal information stored by Equifax.

The complaint stated: "In an attempt to increase profits, Equifax negligently failed to maintain adequate technological safeguards to protect Ms. McHill and Mr. Reinhard's information from unauthorized access by hackers. Equifax knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach. Equifax could have and should have substantially increased the amount of money it spent to protect against cyber-attacks but chose not to."

The class will seek as much as $70 billion in damages nationally.

~30~