Security Now! #547 - 02-16-16

GRC is DOWN

This week on Security Now!

- GRC is DOWN
- A newly discovered, 8-year old, deeply buried buffer overflow
- More on Error 53
- A quick reminder about GWX and more on CheesusChrust
- A wonderful reality check from Bruce Schneier
- James Clapper's IoT comment
- A new ultra-Archive technology
- A bit of errata and miscellany
- Discussion of ECDH key stealing

A Digital Readout Sundial!

https://www.etsy.com/listing/248715228/digital-sundial

Security News

GNU C Library (glibc) "getaddrinfo" stack-based buffer overflow

- https://googleonlinesecurity.blogspot.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html
- https://www.gnu.org/software/libc/

"Overview"
Any Unix-like operating system needs a C library: the library which defines the "system calls'' and other basic facilities such as [file or device] open, malloc, printf, exit…

The GNU C Library is used as *the* C library in the GNU system and in GNU/Linux systems, as well as many other systems that use Linux as the kernel.

The Linux Kernel + the GNU C Library form the Linux API

All the versions of glibc since v2.9.

- The code that causes the vulnerability was introduced in May 2008 as part of glibc 2.9.
- v2.9 was released in November 2008!

Google's Online Security Blog:
<quote> Have you ever been deep in the mines of debugging and suddenly realized that you were staring at something far more interesting than you were expecting? You are not alone! Recently a Google engineer noticed that their SSH client segfaulted every time they tried to connect to a specific host. That engineer filed a ticket to investigate the behavior and after an intense investigation we discovered the issue lay in glibc and not in SSH as we were expecting.

Thanks to this engineer’s keen observation, we were able determine that the issue could result in remote code execution. We immediately began an in-depth analysis of the issue to determine whether it could be exploited, and possible fixes. We saw this as a challenge, and after some intense hacking sessions, we were able to craft a full working exploit!

In the course of our investigation, and to our surprise, we learned that the glibc maintainers had previously been alerted of the issue via their bug tracker in July, 2015. (bug). We couldn't immediately tell whether the bug fix was underway, so we worked hard to make sure we understood the issue and then reached out to the glibc maintainers. To our delight, Florian Weimer and Carlos O’Donell of Red Hat had also been studying the bug’s impact, albeit completely independently! Due to the sensitive nature of the issue, the investigation, patch creation, and regression tests performed primarily by Florian and Carlos had continued “off-bug.”

This was an amazing coincidence, and thanks to their hard work and cooperation, we were able to translate both teams' knowledge into a comprehensive patch and regression test to protect glibc users.

WHAT:
Our initial investigations showed that the issue affected all the versions of glibc since 2.9. You should definitely update if you are on an older version though. If the vulnerability is detected, machine owners may wish to take steps to mitigate the risk of an attack.

The glibc DNS client side resolver is vulnerable to a stack-based buffer overflow when the getaddrinfo() library function is used. Software using this function may be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack.

The "getaddrinfo()" function is used for DNS lookup. Due to a mismanagement of the receiving buffers, the replies from parallel A and AAAA (IPv4 and IPv6) queries may overwrite the receiving buffers.

The Patch:
https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html
Main Conclusions:
Via getaddrinfo with family AF_UNSPEC or AF_INET6 the overflowed buffer is located on the stack via alloca (a 2048 byte fixed size buffer for DNS responses).

At most 65535 bytes (MAX_PACKET) may be written to the alloca buffer of 2048 bytes. Overflowing bytes are entirely under the control of the attacker and are the result of a crafted DNS response.

Local testing shows that we have been able to control at least the execution of one free() call with the buffer overflow and gained control of EIP. Further exploitation was not attempted, only this single attempt to show that it is very likely that execution control can be gained without much more effort. We know of no known attacks that use this specific vulnerability.

Mitigating factors for UDP include:

- A firewall that drops UDP DNS packets > 512 bytes.
- A local resolver (that drops non-compliant responses).
- Avoid dual A and AAAA queries (avoids buffer management error) e.g.
- Do not use AF_UNSPEC.
- No use of `options edns0` in /etc/resolv.conf since EDNS0 allows responses larger than 512 bytes and can lead to valid DNS responses that overflow.

- No use of `RES_USE_EDNS0` or `RES_USE_DNSSEC` since they can both lead to valid large EDNS0-based DNS responses that can overflow.

Mitigating factors for TCP include: Limit all replies to 1024 bytes.

The code that causes the vulnerability was introduced in May 2008 as part of glibc 2.9.

A back of the envelope analysis shows that it should be possible to write correctly formed DNS responses with attacker controlled payloads that will penetrate a DNS cache hierarchy and therefore allow attackers to exploit machines behind such caches.

Error 53:
Dale Perkel @PerkX #error53
Steve, I'm an InfoSec professional during the day and an independent Apple repair business at night. In South Africa where I live, there's very little official Apple support, except possibly from the mobile operators who charge huge amounts and generally repair time is on the order of 2 weeks.

I offer an overnight service at an affordable price and hence have repaired hundreds of Apple devices in the past 2 years.

Error 53 is extremely frustrating, as there are legitimate reasons to replace the TouchID sensor, such as accidental / liquid damage or failure of the home button mechanism.

I always advise my customer that this will void the warranty (if there is one) and TouchID will be disabled, to which they consent.

Why, when an update is installed weeks or months later, should the iPhone be irrevocably "bricked" with no possibility of recovering data? If there were criminal or unauthorized access attend, surely the attacker wouldn't take the opportunity to upgrade to the latest iOS? The window of opportunity is essentially infinite for a determined attacker.

Why can the iOS update not just detect the missing or changed fingerprint reader and destroy the contents of the secure enclave without turning the entire iPhone into a very expensive paper weight?

I trust Apple to provide the best possible security and they rarely fail. But this is akin to needing to buy a new car if you loose your car keys... Thanks for the great show, I look forward to it every week! Cheers, Dale

Bad Apple. The Intentional Bricking of Working iPhones with Error 53 (Feb 7th)
http://mendonipadrehab.com/entries/general/bad-apple-the-intentional-bricking-of-working-iphones-with-error-53
iPadRehab / Smartphone & iDevice Repair
https://www.youtube.com/watch?v=Enkyc7phATc

Is a phone with a new home button less secure?
No. Aftermarket home buttons have no fingerprint sensor at all. They are just home buttons. A phone with a new home button will simply have anything related to touch ID greyed out, the sensor is not there. It cannot be accessed by Touch ID of the button. Apple Pay will not respond with the fingerprint. The phone is still secured (if the consumer wishes) by the passcode lock just as all phones. If the phone is stolen, it cannot be reset and activated without the original owner's Apple ID and password--i.e. it is protected from theft with the iCloud activation lock.

But it will work. Indefinitely. You can enjoy all the other functions of the phone. You can call, and text, take selfies, connect to WiFi and check email. You can play Candy Crush and FaceTime and surf the internet. It is a perfectly functional phone, no different in any way from say, my iPhone 6. I think touch ID is annoying and I've never even set it up. I choose not to use that feature of the phone.

But then one day you click "ok" in response to Apple constantly bugging you to update your iOS. The result? The phone chugs along and then fails to update with error 53. You can not go back in time and 'undo' this failed update. Your phone will boot to recovery mode and there is no escape. The special pictures you took that morning are gone. Your notes and grocery list are gone. The phone you paid $700 for is now a complete brick. The phone itself has no hardware defect, it simply can't answer the question from the CPU with "yes I am here" from the fingerprint sensor chip. There is no recourse. Apple has intentionally bricked your working iPhone 6.

Microsoft's No GWX:
Via Twitter: On the last SN, you mentioned some Windows updates that prevent Win7 from ever updating to Win10. I can't find these. Do you have a link, or did I misunderstand? Thanks!
http://bit.ly/no-gwx

More on Windows 10 Internet Connections

http://www.zdnet.com/article/when-it-comes-to-windows-10-privacy-dont-trust-amateur-analysts/

Ed Bott weighs in knowledgeably on the Forbe's coverage of "CheesusChrust"
Ed Notes that in addition to the user-facing pages of disabling...
<quote> Actual network administrators configuring Windows 10 Enterprise have hundreds of Group Policy options at their disposal, including fine-grained controls over telemetry and privacy settings. There's even a fourth option, not available to users of retail and OEM Windows 10 editions, that dials telemetry back to an absolute minimum. There is no evidence that Mr. Crust is aware of these options.

And then, Mr. Crust reports, he "configured the DD-WRT router to drop and log all connection attempts via iptables through the DD-WRT router by Windows 10 Enterprise."

Bruce Schneier's Worldwide Encryption Product Survey

https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html

(A PERFECT wake-up call for our clueless US legislators.)
Today I released my worldwide survey of encryption products.

The findings of this survey identified 619 entities that sell encryption products. Of those, 412, or two-thirds, are outside the U.S.-calling into question the efficacy of any US mandates forcing backdoors for law-enforcement access.

It also showed that anyone who wants to avoid US surveillance has over 567 competing products to choose from. These foreign products offer a wide variety of secure applications -- voice encryption, text message encryption, file encryption, network-traffic encryption, anonymous currency -- providing the same levels of security as US products do today.

Details:

There are at least 865 hardware or software products incorporating encryption from 55 different countries. This includes 546 encryption products from outside the US, representing two-thirds of the total.

The most common non-US country for encryption products is Germany, with 112 products. This is followed by the United Kingdom, Canada, France, and Sweden, in that order.

The five most common countries for encryption products -- including the US -- account for two-thirds of the total. But smaller countries like Algeria, Argentina, Belize, the British Virgin

Islands, Chile, Cyprus, Estonia, Iraq, Malaysia, St. Kitts and Nevis, Tanzania, and Thailand each produce at least one encryption product.

Of the 546 foreign encryption products we found, 56% are available for sale and 44% are free. 66% are proprietary, and 34% are open source. Some for-sale products also have a free version.

At least 587 entities -- primarily companies -- either sell or give away encryption products. Of those, 374, or about two-thirds, are outside the US.

Of the 546 foreign encryption products, 47 are file encryption products, 68 e-mail encryption products, 104 message encryption products, 35 voice encryption products, and 61 virtual private networking products.

The Guardian: US intelligence chief: we might use the internet of things to spy on you
http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper
<PHOTO>
The US intelligence chief has acknowledged for the first time that agencies might use a new generation of smart household devices to increase their surveillance capabilities.

As increasing numbers of devices connect to the internet and to one another, the so-called internet of things promises consumers increased convenience – the remotely operated thermostat from Google-owned Nest is a leading example. But as home computing migrates away from the laptop, the tablet and the smartphone, experts warn that the security features on the coming wave of automobiles, dishwashers and alarm systems lag far behind.

In an appearance at a Washington thinktank last month, the director of the National Security Agency, Adm Michael Rogers, said that it was time to consider making the home devices "more defensible", but did not address the opportunities that increased numbers and even categories of connected devices provide to his surveillance agency.

However, James Clapper, the US director of national intelligence, was more direct in testimony submitted to the Senate on Tuesday as part of an assessment of threats facing the United States.

Clapper said: "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."

New "5D" super-archival recording technology

- To be presented tomorrow at the Society for Optical Engineering Conference in San Francisco.
- '5D Data Storage by Ultrafast Laser Writing in Glass'
- http://www.southampton.ac.uk/news/2016/02/5d-data-storage-update.page
- Scientists at the University of Southampton have made a major step forward in the development of digital data storage that is capable of surviving for billions of years.

  Using nanostructured glass, scientists from the University's Optoelectronics Research Centre (ORC) have developed the recording and retrieval processes of five dimensional (5D) digital data by femtosecond laser writing.

  The storage allows unprecedented properties including 360 TB/disc data capacity, thermal stability up to 1,000°C and virtually unlimited lifetime at room temperature (13.8 billion years at 190°C) opening a new era of eternal data archiving. As a very stable and safe form of portable memory, the technology could be highly useful for organisations with big archives, such as national archives, museums and libraries, to preserve their information and records.
- "Self-Assembled nanostructures" created in fused quartz.
- 5D -- structure size and orientation + 3D location.

Errata

- Not "Text-to-Speech" (TTS) but rather "Speech Recognition"

- DangerDad (@emarkp) @SGgrc ICYMI the German stellarator was at 80 MILLION, not 80 BILLION degrees. And has 5-fold symmetry.

Miscellany

Zeo Update:

- 100, 355, 460 (915)
- 1,197 of the final round sold
- Zeo's Open-Source API -- Call For Developers!

Digital Sundial

- https://www.etsy.com/listing/248715228/digital-sundial
- SN's Photo of the Week

SpinRite

<<name withheld by request>>
Location: Beirut, Lebanon
Subject: Files gone from hard disk
Date: 14 Feb 2016 23:45:02
:
Hello Steve,
I have a 2 year old desktop that suddenly started causing problems. For example, it would show the recover the windows option during boot sometimes, and sometimes it would just boot normal. After couple of times, the recovery option started popping up every time and all the recovery options were of no use. I took the hard disk off the desktop and connected to my laptop using a sata usb extension to get the data out of it. At this point, to my surprise, some data were present and some others were not. Even though I was sure the data were there and I have not deleted them. Is this even possible? I mean, do bad sectors cause data to just disappear? I ran a recovery software to check if the files were deleted, and it found nothing. What would possibly have gone wrong? How would spinrite help in such a scenario? Thank God I had a very recent back up and just lost 3 days of work.

(In case you are going to talk about this on SN, I would appreciate if you do not disclose my name)

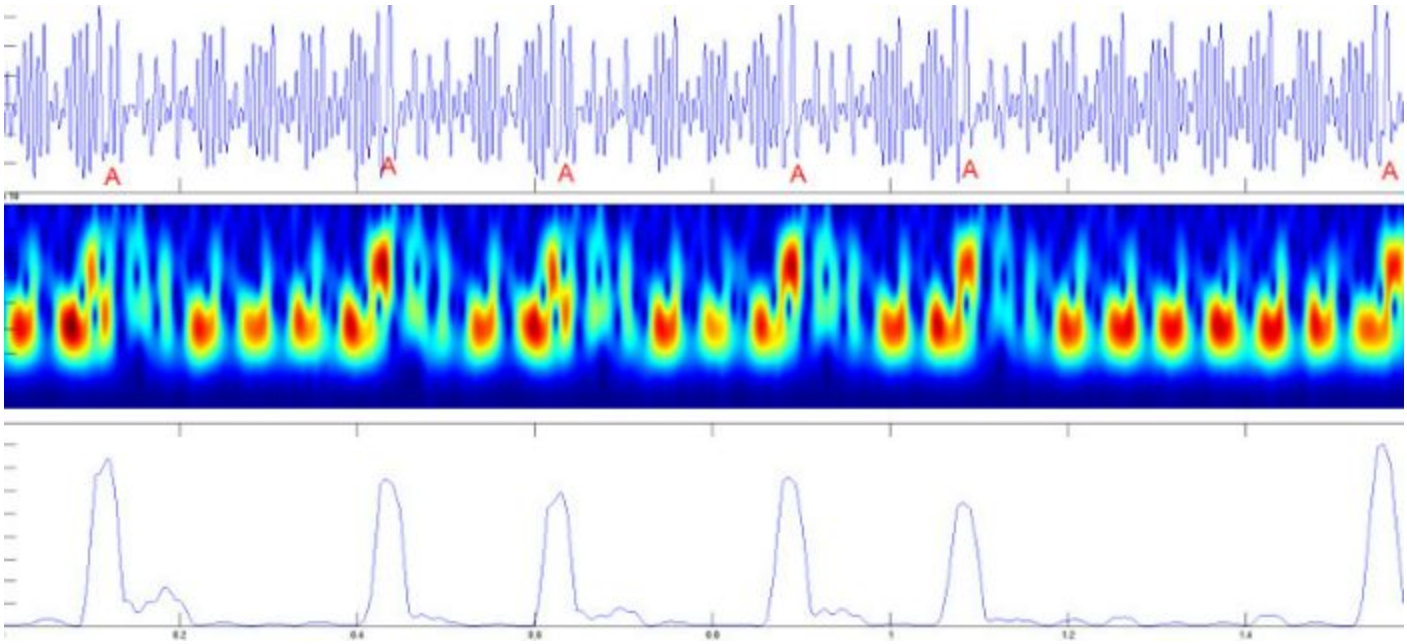
Thanks a lot,
regards

(All SpinRite v6.0 owners will move to v6.1 for free!)

Stealing ECDH Keys

- http://motherboard.vice.com/read/how-white-hat-hackers-stole-crypto-keys-from-an-offline-laptop-in-another-room
- http://eprint.iacr.org/2016/129.pdf
- http://www.cs.tau.ac.il/~tromer/ecdh/


Aaronia MDF
24.2 0.34
15.7 0.08



We show that the secret decryption keys can be extracted from PCs running the the ECDH encryption algorithm, using the electromagnetic emanations generated during the decryption process. By measuring the target's electromagnetic emanations, the attack extracts the secret decryption key within seconds, from a target located in an adjacent room across a wall.

ECDH (Elliptic Curve Diffie Hellman) is a standard public-key encryption algorithm used in OpenPGP, as specified in RFC 6637 and NIST SP800-56A. We attacked the ECDH implementation of GnuPG's libgcrypt 1.6.3 (the latest version at the time the paper was written). The attack asks for decryption of a single carefully-chosen ciphertext, iterated a few dozen times, and then uses time-frequency signal analysis techniques in order to extract from the electromagnetic leakage emitted by the target laptop during execution of ECDH decryptions.

Q&A

Q1: How vulnerable are GnuPG and other applications that use libgcrypt now?

We have disclosed our attack to GnuPG developers under CVE-2015-7511 and worked with the developers to implement countermeasures. GnuPG's Libgcrypt 1.6.5, containing these countermeasures and resistant to the key-extraction attack described here, was released concurrently with the public posting of these results.

Specifically, Libgcrypt 1.6.5 completely changed their implementation of the elliptic-point curve multiplication, to the "double-and-always-add" algorithm. This is slower than the prior implementation, but more resistant to side-channel attack since the sequence of high-level arithmetic operations does not the depend on the secret key.

Q4: What if I can't get physically close enough to the target computer?

For RSA and ElGamal (though not yet for ECDH), similar attacks have been demonstrated from large distances:

- *Laptop-chassis potential*, measured from the *far end* of virtually any shielded cable connected to the laptop (such as Ethernet, USB, HDMI and VGA cables) can be used for key-extraction, as we demonstrated in a paper presented at CHES'14.
- *Acoustic emanations (sound)*, measured via a microphone, can also be used to extract keys from a range of several meters, as we showed in a paper presented at CRYPTO'14.