Security Now! #786 - 09-29-20

ZeroLogon++

This week on Security Now!

This week we look back at the just-release Chrome 85. We see that an enterprise's choice of VPN gateway really does make a difference. We drop in for an update on what would have to be called the new ransomware gold rush, and we examine the implications of Ring's latest announcement of their flying spy drone — I mean webcam. Then we learn how much Vitamin D Dr. Fauci takes, and invite our podcast listeners to lock down their UserID of choice at GRC's new web forums using a non-public URL. Then we conclude with the required big update to the ZeroLogon story which we began last week.

Browser News

Chrome's v85.0.4183.121 Release

Last week we noted that Chrome was right on the brink of updating to 85, but we didn't yet have all the details. And since several of the things that were fixed were extremely serious remote code execution vulnerabilities, we still don't have all the details, and Google won't be releasing them until they have lost their value as attack vectors once everyone has been updated. These are not 0-days, in that Google stated that they are not aware of any of these being used in the wild. Which is not the same as knowing that they are not, but it's all we've got.

As we've observed, that updating process often occurs during a “roll-out” that can take some time, and Google's “Chrome Releases” document page about this last week starts out by saying: “The stable channel has been updated to 85.0.4183.121 for Windows, Mac, and Linux, which will roll out over the coming days/weeks.” So it might be awhile.

Some of the things that were fixed were vulnerabilities that could have enabled zero-click remote code execution on a visitor's machine by simply visiting a hostile site that was aware of and had weaponized the vulnerability. We don't know, yet, but it might have been deliverable via “malvertising.”

Overall, 10 security flaws were fixed. And I was glad to see that the top two disclosures earned their discoverers $15K each, with the third being rewarded $10K. This bug bounty model — and relying upon the ethics of those who discover such problems — has become a crucial aspect of today's threat management landscape. I mention ethics here, because a weaponizable, zero-click, unknown, remote code execution exploit for the world's leading web browser — by a large margin — could doubtless have been sold to the likes of Zerodium for a far higher price. So, while it's terrific that Google, like a growing number of other companies, is paying for important disclosures, the dark underbelly remains the highest bidder. So we're also depending upon the ethics of those who appreciate the destructive power of their discoveries.

https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html

I've placed a link to the release report in the show notes. I tried to drill down to get additional information on the individual issues, but the pages all came up “Permission denied” with a banner across the top reading: “Chromium Googlers, we're investigating a problem with issue permissions: http://crbug.com/monorail/8426” So, no additional information was readily available.

For now, all we can do is to make sure that any desktop Chrome we're using is at v85, and be glad that those problems were found and eliminated before their use was observed in the wild.

Security News

The VPN you choose DOES make a difference.

From time to time, through the years, we've had various recommendable VPN service providers as sponsors of the TWiT Network. Our argument then, has been that the provider you choose does make a difference. This bit of news offers an example of just that: https://securingsam.com/breaching-the-fort/

Two researchers who work for a network security platform provider “SAM Seamless Network” introduced their most recent discovery by explaining:

> Many have written, and probably more will be told about the dramatic change in the way each of us works remotely following the Covid-19 pandemic. As security researchers, we have been trying to assess whether the existing security solutions address the new situation. We noticed that many companies are resulting in requiring employees to connect to the office via VPN. Whether it’s because of on-site data centers or IP anchoring, many small businesses (less than 20 employees) use a VPN server that is usually also the company’s gateway. Not too long after we began our research, the name FortiGate was thrown into the air. We instantly grabbed the FortiGate that we kept as a backup in the office and began exploring.
>
> Surprisingly (or not?), we quickly found that under default configuration the SSL VPN is not as protected as it should be, and is vulnerable to MITM attacks quite easily. The Fortigate SSL-VPN client only verifies that the CA was issued by Fortigate (or another trusted CA), therefore an attacker can easily present a certificate issued to a different Fortigate router without raising any flags, and implement a Man-In-The-Middle attack.
>
> We searched and found over 200,000 vulnerable businesses in a matter of minutes.

So the scenario is, employees have moved home in droves and are now connecting back to their corporate network over the popular FortiGate VPN gateway. Perhaps a quite recently deployed FortiGate gateway. They describe an entirely feasible scenario where a compromised IoT device in the remote user's home is able to use ARP poisoning to intercept the employee's connection to the corporate VPN gateway and insert itself into the loop. They’re IoT security folks, so they take the “evil IoT device” attack model. In practice, such interception could be performed anywhere along the path from employee to their corporate VPN. A bonanza could be had by a serious entity — say a corporate espionage competitor — arranging to intercept their competitor's bandwidth close to, but outside of, the company.

The essence of the flaw that was discovered was that any device or attacker who can arrange to intercept the client's remote connection can relay their authentication to the corporate FortiGate gateway, despite its being protected by a VPN.

The FortiGate VPN Gateway is an SSL-VPN. So it establishes a standard SSL/TLS connection using the client and server model we’re all quite familiar with. To that end, every FortiGate VPN gateway has a unique certificate, where the certificate's Common Name (CN) consists of the model number and serial number of that device. Since every serial number is unique, every certificate is unique.

The trouble arises, as these guys noted, because the FortiGate VPN CLIENT, when used with its default settings, does not bother to check whether it's connecting to the CORRECT FortiGate VPN. It doesn't look at the connecting certificate's name at all. It doesn't bother to check that it's connecting to ANY FortiGate VPN Gateway. If the certificate is valid and has been signed by any valid and recognized certificate authority, that's good enough for the FortiGate client!

In other words, this would be like having our web browsers not even looking at the name on server certificates when our browsers connect to remote web servers offering them. All that would be checked was that the certificate itself was valid and it was signed by someone valid. We all know that would be totally nuts, since any sort of attack to intercept or reroute traffic — like intercepting DNS — would allow an attacker to spoof the remote web server's identity.

So, the FortiGate VPN offers ZERO protection against man-in-the-middle (MITM) interception. An attacker (even an IoT lightbulb on the home user's LAN) simply answers the client's TLS connection with a valid certificate — any valid certificate. The attacker simultaneously reaches out to the FortiGate VPN Gateway and initiates its own fresh incoming connection. When the user's client sends its authentication credentials, it's the attacker who receives them (probably records them) and then forwards them to the connection it has made to the corporate gateway. The attack then proceeds with the attacker having access to the decrypted content of everything that moves back and forth. And note that the attacker is now also on the corporate LAN under the user's credentials. So it can get up to all manner of other mischief while the client is online and none and wiser.

The problem is bad and the fix it trivial: If the client were simple configured to verify the Gateway's certificate by name, and require that it be signed by the FortiGate Certificate Authority and no other, whose root certificate would have been installed at client setup, then any intercepting man in the middle would be locked out since they could not authenticate to the client with a FortiGate VPN server certificate... which they could never have.

The only way to explain this clearly insecure configuration for a VPN would be that all of the concern must have been about the client authenticating themselves to the corporate LAN — that's necessary but not sufficient. The clear need to have the gateway also authenticate to the client was apparently somehow missed.

Being responsible lads, the researchers reached out to the Fortinet folks to share what they had found and to get their comments. FortiGate reportedly responded that they are well aware of it, but are not going to change it. They claim that since the user has the ability to manually replace the certificate that was provided with the system, it's the user's responsibility to make sure the connection is protected. Wow. And the SAM Seamless Network guys noted in their write-up that <quote> "Moreover, there is no clear warning by Fortinet to the user, that this major security flaw exists when using the default certificate. Instead, a vague message is displayed."

They concluded their posting: "We decided to take the research a step further, and check how many Fortinet devices are vulnerable to this type of attack. Using the Shodan.io database, we found ~230k Fortigate devices that are using the VPN functionality. Out of these, roughly 88%, that is over 200k (!) businesses are using the default configuration and can be easily breached using any man-in-the-middle method."

Wow. One of my favorite aphorisms on this podcast is “The Tyranny of the Default.” Fortinet's defense that their gateway CAN be made secure is horrifying when you consider the security that any purchaser would assume they are obtaining. What else are they buying? And the numbers shown from the Shodan scan — that, indeed, 88% of all identified installations **are** using the insecure default — demonstrates that Fortinet is badly letting their customers down.

A “Ransomware Goldrush”

Bleeping Computer, who has, as we know, been intensely focused upon the ransomware world since it first emerged onto the info security scene, used the term “Ransomware Goldrush” to describe the past week. Lawrence Abrams has assembled a timeline of events occurring during just a recent 7-day period from the 19th through the 25th, and I want to give everyone a sense for what's actually going on out there...

September 19th:

Michael Gillespie and PolarToffee found a new ransomware called Egregor that appears to be a Sekhmet spinoff. It uses a random extension and drops a ransom note named RECOVER-FILES.txt.~

Recall that Michael Gillespie is the guy who has been reverse engineering those poorly written but still effective Ransomware strains that permit some hope for non-ransom payment decryption. His pages over at Bleeping Computer now contain decryptors for 23 different ransomware variants.
https://www.bleepingcomputer.com/download/windows/ransomware-decryptors/

Michael Gillespie found a new variant of the LeakThemAll ransomware that appends .montana and drops a ransom note of !HELP!.txt.

GrujaRS found a new ransomware that appends the .zhen extension to encrypted files.

September 20th 2020:

Michael Gillespie found a new variant of the STOP ransomware that appends the .kolz extension to encrypted files.

September 21st 2020

A ransomware named ThunderX was recently discovered. After its analysis, for those fortunate enough to look for it, a ransom-free decryptor has been created. The trouble is, many victims won’t know to look for it.

Meanwhile, also last Monday the 21st, Nathan Wyatt, previously known as the ‘Dark Overlord’ hacker pleaded guilty and was sentenced to 5 years in prison for his extortion threats where he was threatening to publicly release information from hacking victims unless they agreed to his digital extortion demands.

Last Monday Michael Gillespie found a new ransomware that appends the .encrypted extension and drops a ransom note named SOLVE ENCRYPTED FILES.txt.

He also found a new variant of the Matrix Ransomware that appends the .JB88 extension and drops a ransom note JB88_README.rtf.

Xiaopao found new Nefilim variant that appends the .TRAPGET extension and drops a ransom note named TRAPGET-INSTRUCTION.txt.

September 22nd 2020

Luxottica, the Italian owner of the Ray-Ban brand, has confirmed that they were the victim of a ransomware attack which has disrupted work, shutting down operations in Italy and China.

Meanwhile — and this is really interesting — a provider of cyber insurance has begun performing security scans during their initial underwriting phase. So they're saying "Yeah, we'll agree to cover you, but first we're going to check your security to see if we find anything obviously wrong." Since they've been doing this they are reporting a 65% reduction in subsequent ransomware claims being made against their clients.

Michael Gillespie found a new Matrix variant that appends the .FG69 extension and drops a ransom note named FG69_README.rtf.

Xiaopao found a new Matrix ransomware variant that appends the .AW46 extension and drops a ransom note named !AW46_INFO!.rtf.

GrujaRS found a new ransomware that appends the .CRPTD extension to encrypted files.

3xp0rt found a ransomware actor selling a complete ransomware kit for $2,000.

September 23rd 2020

A leading government technology services provider Tyler Technologies has suffered a ransomware attack that has disrupted its operations.

We've talked about the problems QNAP NAS devices have been having. Now they've been targeted by the AgeLocker ransomware, which encrypts the device's data, and in some cases, steals the victim's files.

A new ransomware group has been targeting large corporate networks using backdoors of their own design and file-encrypting malware for the initial and final stages of the attack.

Joakim Kennedy found a new ransomware written in Golang that is pretending to be REvil. What's odd about it is that there's no way for its victims to recover any files since there's no contact information provided. So researchers think that perhaps it's just a wiper.

September 24th 2020

A new ransomware campaign named “Mount Locker” is underway. It exfiltrates its victims' files before encrypting them, and is then demanding multi-million dollar ransoms.

S!ri found the new Dusk v1.0 Ransomware that drops a ransom note named !#!READ-ME!#!.txt

JAMESWT found a sample of the new Exorcist 2.0 ransomware.

September 25th 2020

Michael Gillespie found a new Stop variant that appends the .copa extension to encrypted files.

He also found a new Matrix variant that appends the .DEUS extension and drops a ransom note named DEUS_INFO.rtf.

So, there’s just one week in the ransomware world. It should give everyone a sense for just how totally crazy and out of control this new bitcoin-enabled cyber-extortion

But wait!... there’s more!

REvil ransomware gang deposited $1 million of bitcoin a in hacker recruitment drive

The REvil Ransomware (Sodinokibi) operation has deposited $1 million in bitcoin onto a Russian-speaking hacker forum to demonstrate to potential affiliates that they mean business... meaning that there is money to be made by joining their affiliate program.

Backing up a bit... as we covered when it happened, an increasing number of ransomware operations are being conducted as a Ransomware-as-a-Service (RaaS), where the ransomware developers develop and provide the ransomware and also maintain and run the extortion payment site, and then affiliates are recruited to hack into businesses and encrypt their data.

The ransomware developers typically receive a modest 20% to 30% cut, and an affiliate gets the balance 70% to 80% of whatever ransom payment is received.

At one point the REvil gang had closed their site to new affiliates, stating that they had all they needed. That changed yesterday when the gang announced that they were once again recruiting new affiliates to distribute their ransomware. Their posting indicates that they are seeking teams of skilled hackers at penetration testing, or experienced individuals.

1. Teams that already have experience and skills in penetration testing, working with msf / cs / koadic, nas / tape, hyper-v and analogues of the listed software and devices;

2. People who have experience, but do not have access to work;

And, as I noted at the top, to show potential affiliates that they mean business, REvil has deposited 99 bitcoins, or approximately $1 million, on the hacker forum. This particular hacker forum allows members to deposit bitcoins into a wallet hosted by the site. Members can see other members' deposits, and the deposited bitcoins can be used to privately buy and sell illicit services or data through the forum. As of this posting, REvil now has 99 bitcoins deposited and on view on the hacker forum.

This deposit is meant to illustrates how much money ransomware operations are generating since they are publicly making a $1 million deposit as if it is not a big deal. And this deposit also shows that they're not very concerned that the forum administrators could steal it. Since the hacker forum's owner manages the members' bitcoin wallets, the owner could pull an exit scam and abscond with the bitcoins.

Unfortunately, Ransomware is here to stay.

Remember the Ryuk ransomware?

And over this past weekend, starting last Saturday night to better avoid detection, the huge international, 400-healthcare facility Universal Health Services, currently in 330th place on the Forbes 500 list of the largest US publicly traded companies, was hit by a huge Ryuk ransomware attack.

Early Sunday morning they shut down systems at healthcare facilities around the US. Based up reports from UHS' employees, UHS hospitals in the US including those from California, Florida, Texas, Arizona, and Washington D.C. are left without access to computer and phone systems. And at the moment the affected hospitals are redirecting ambulances and relocating patients in need of surgery to other nearby hospitals.

One of the reports said: “When the attack happened multiple antivirus programs were disabled and hard drives just lit up with activity. After 1 minUte or so of this, the computers logged out and shutdown. When you try to power back on, the computers just automatically shut back down. We have no access to anything computer based including old labs, EKG's, or radiology studies. We have no access to our PACS radiology system.”

Employees were told to shut down all systems to block the attackers' from reaching further devices on the network.

And, sadly, four deaths have now been ascribed to the incident due to doctors needing to wait for lab results to arrive via courier since all electronic channels were down.

Reports are that during the cyberattack, files were being renamed to include the .ryk extension — the Ryuk ransomware hallmark.

Based on some information that was shared with BleepingComputer by Vitali Kremez of “Advanced Intel”, the attack on UHS' system likely started through a phishing attack.

According to Vitali, their Andariel intelligence platform detected both the Emotet and TrickBot Trojans affecting UHS Inc. throughout 2020, and more recently, this month. The Emotet trojan is spread via phishing emails containing malicious attachments that install the malware on a victim's computer. After some time, Emotet will also install TrickBot, which ultimately opens a reverse shell to the Ryuk operators after harvesting sensitive information from compromised networks.

Once the Ryuk actors manually get access to the network, they start with reconnaissance and, after gaining admin credentials, they deploy ransomware payloads on network devices using PSExec or PowerShell Empire.

In other words, the WAY this is being done is well understood and is no mystery at all. But much like the APT threat that gave Sony Entertainment so much trouble years ago, it's virtually impossible to secure anything that's as sprawling as a 400 facility network where everyone has PCs with eMail.

UHS put out a public statement:

> The IT Network across Universal Health Services (UHS) facilities is currently offline, due to an IT security issue.
>
> We implement extensive IT security protocols and are working diligently with our IT security partners to restore IT operations as quickly as possible. In the meantime, our facilities are using their established back-up processes including offline documentation methods. Patient care continues to be delivered safely and effectively.
>
> No patient or employee data appears to have been accessed, copied or otherwise compromised.

The Flying Webcam

Under our rhetorically-named “What could possibly go wrong?” section we have Amazon/Ring's announcement last Thursday of their autonomous, home security, flying webcam. It will be named the “Always Home Cam” at a cost of $250 and is slated to start shipping next year.

It is self-docking to recharge and can autonomously fly around its owner's home on pre-approved paths. This is supposed to allow homeowners to check to see if they left a window open, forgot to turn the stove off, or to check to make sure robbers aren’t breaking in.

And perhaps not surprisingly, this announcement has been met with some mixed feelings. Rick Holland, the CISO and VP of Strategy at Digital Shadows, told Theatpost: “For privacy advocates, the concept of an untethered IoT device surveilling the house is disturbing. Coupled with Ring’s controversial privacy practices, the adoption of the drone could be low. However, those that have already embraced the concept of in-house security cameras are likely to be excited. The prospect of having a single drone monitor your house instead of multiple individual cameras could be alluring.”

Ring for its part said that it has built privacy features into the physical design of the Always Home Cam. When the drone is docked in its charging base, the camera is physically blocked. The device has also been designed to hum at a certain volume, so it’s clear that the camera is in motion and recording.

Wait... Hum??!! Are you kidding me? Has anyone here NOT ever heard a micro drone fly?

You can't hear yourself think!! Generating the lift required using four tiny designer-approved props requires that they spin at thousands of revolutions per minute. At least I suppose we won't need to worry about this flying menace creeping up on and surprising anyone.

What I want to know is whether no one who designs and tests these things has a dog or cat at home, because this thing will drive them insane and right under the bed, never to emerge.

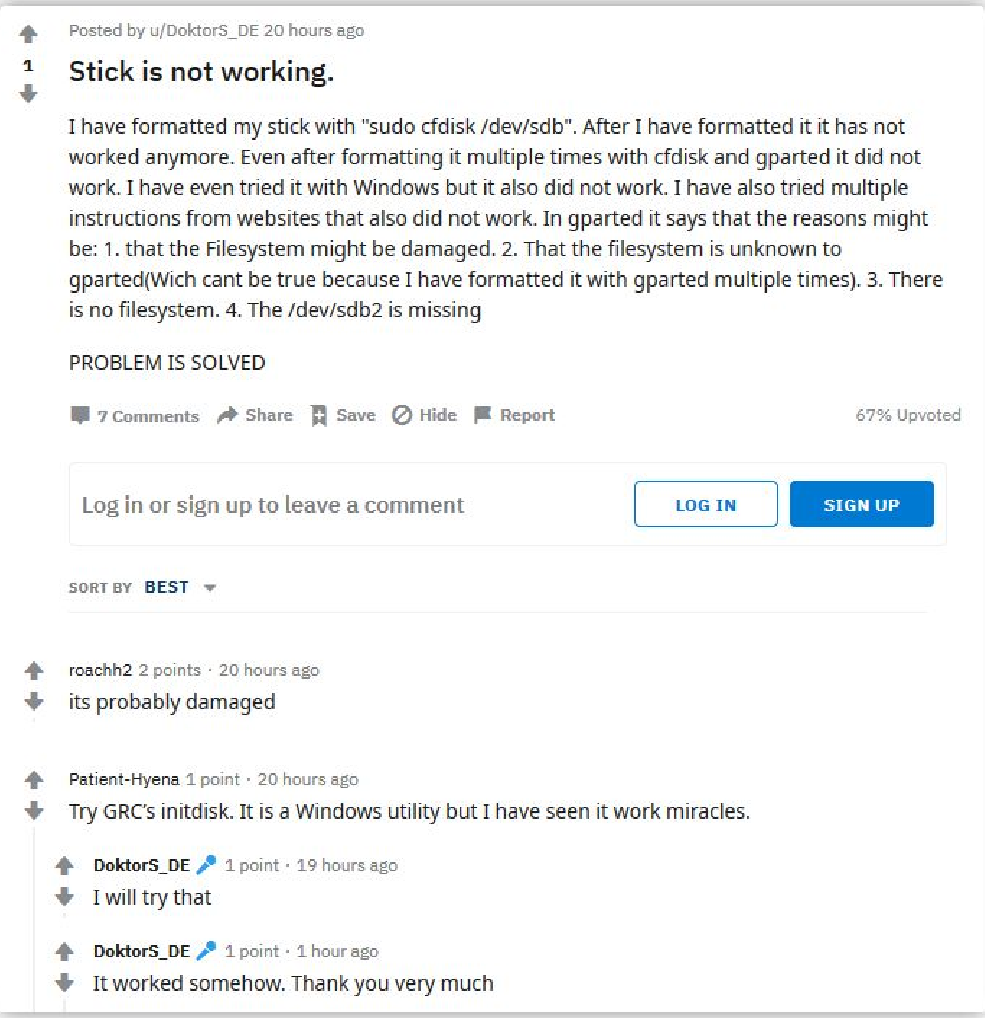
Which us to another of this podcast's favored aphorisms: "Not everything that can be done, should be done."

Health

Dr. Fauci reports taking 6,000 IU of Vitamin D per day.
https://www.youtube.com/watch?v=ZqZLMoLvhgk
(Can we play the first 3 minutes of this into the podcast?)

InitDisk

https://www.reddit.com/r/linuxquestions/comments/j1kiod/stick_is_not_working/



Posted by u/DoktorS_DE 20 hours ago

Stick is not working.

I have formatted my stick with "sudo cfdisk /dev/sdb". After I have formatted it it has not worked anymore. Even after formatting it multiple times with cfdisk and gparted it did not work. I have even tried it with Windows but it also did not work. I have also tried multiple instructions from websites that also did not work. In gparted it says that the reasons might be: 1. that the Filesystem might be damaged. 2. That the filesystem is unknown to gparted(Wich cant be true because I have formatted it with gparted multiple times). 3. There is no filesystem. 4. The /dev/sdb2 is missing

PROBLEM IS SOLVED

roachh2 2 points · 20 hours ago
its probably damaged

Patient-Hyena 1 point · 20 hours ago
Try GRC's initdisk. It is a Windows utility but I have seen it work miracles.

DoktorS_DE 1 point · 19 hours ago
I will try that

DoktorS_DE 1 point · 1 hour ago
It worked somehow. Thank you very much

SpinRite

The new GRC web forums are now fully up and running.

As we've been covering round after round of catastrophic WordPress add-on disasters, I've been growing more and more nervous about hosting a public WordPress blog on my own servers. It's difficult to be convinced of its safety without investing far more in it than I want to. And I'm not a prolific blogger. This podcast audience gets pretty much everything that I have to say every week, and aside from being here with everyone, I work over in GRC's newsgroups. I had only made a single blog posting in years. Thus, the risk/reward ratio of hosting a WordPress presence was all wrong. If I were to do it again, I would go back to letting WordPress host my blog on THEIR server and keep WordPress as far away from my servers as possible. But I realized that I could create a blog forum on GRC's new forum system and have everything integrated and in one place. So that's what I've done. And then with great relief I completely shut down and removed WordPress from my site and sight.

As for the rest of the new web forums, we're still in the staging stage, awaiting the finalization and readiness of the “ReadSpeed” low level driver testing mass storage benchmark -- which I will now be returning to work on finalizing. So there's still not much content there yet and nothing really for anyone to do there. But I'm ready to invite our podcast listeners who would like to register and claim their UserID to do so. It is my intention that these forums will grow to become GRC's, and my own, primary public presence for managing everything I do from now on.

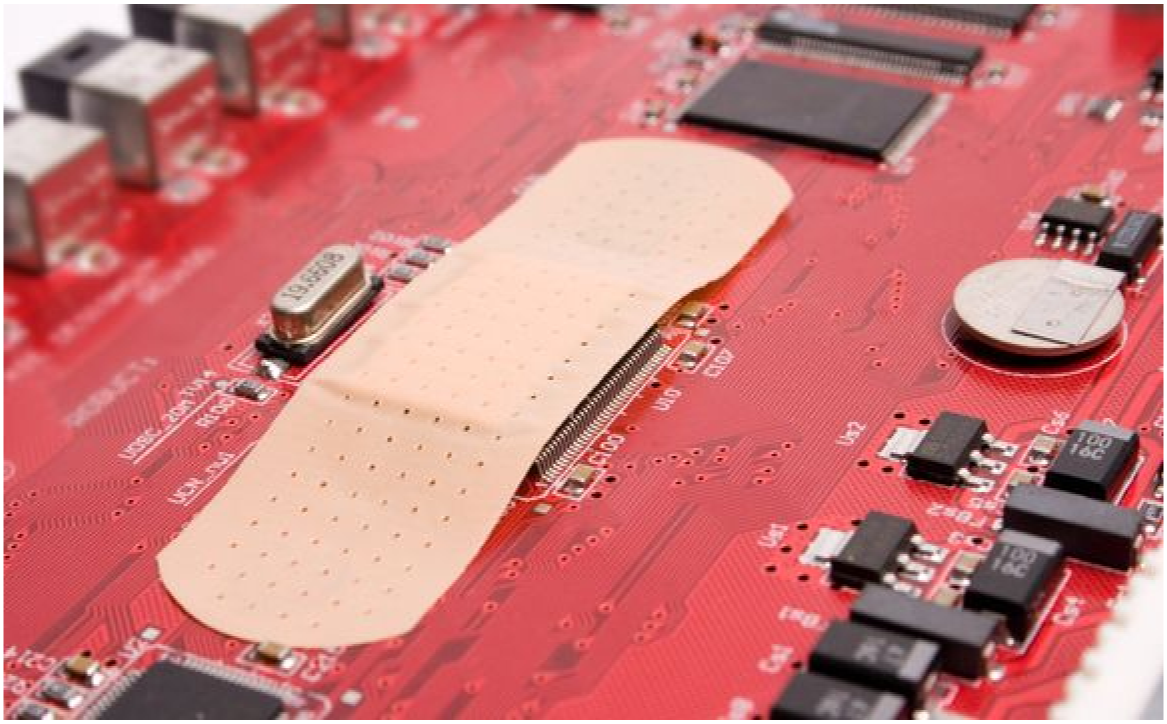
There are still no links to it from GRC and I've removed the forum's obvious registration UI to make it by invitation only. The URL is simply:

http://forums.grc.com/register/

There's no hurry or rush. But everyone listening to this podcast is welcome to register and grab their preferred UserID. Since we all hate eMail spam, I've configured the forum to **never** send any eMail notifications unless specifically requested. So you'll probably want to click the “Watch” button at the top of my blog forum to receive a note when I post news there.

Now it’s back to work to get this extremely interesting benchmark ready for everyone to play with!

ZeroLogon++



Last week one of many topics was the so-called “ZeroLogon” vulnerability. This week it has grown to become this week’s main subject. Last week I introduced us to Secura's earlier discovery and responsible disclosure, which resulted in a quiet patch as part of August's patch Tuesday. Then, six weeks later, having appropriately waited a month and a half, Secura released their full description of the vulnerability. Although they had created a working proof of concept (PoC) demo, they chose to withhold it to allow more time to pass for the August updates to be more widely deployed. But, while withholding for PoC was a nice gesture, the lesson to the industry going forward will be that all anyone needs to turn a nebulous vulnerability description into an exploit is a sufficiently clear description, such as Secura provided. Because within hours of Secura's disclosure multiple working ZeroLogon PoC's has been created, worked out, tested, verified and posted to GitHub.

One week ago when I first talked about this there were three publicly posted exploits on GitHub. Today they are more than the first page of results returned by Google:

ZeroLogon exploitation script
https://github.com/risksense/zerologon

Zerologon test for SMB & RPC (Demonstrates that CVE-2020-1472 can be done via RPC/SMB, and not only over RPC/TCP)
https://github.com/zeronetworks/zerologon

Invoke-ZeroLogon
https://github.com/BC-SECURITY/Invoke-ZeroLogon

ZeroLogon testing script
https://github.com/SecuraBV/CVE-2020-1472

CVE-2020-1472 POC
https://github.com/dirkjanm/CVE-2020-1472

Zer0Dump
https://github.com/bb00/zer0dump
Zer0dump is an PoC exploit/tool for abusing the vulnerabilities associated with CVE-2020-1472 (Zerologon) in order to initiate a full system takeover of an unpatched Windows domain controller.

Zerologon
Checker & Exploit Code for CVE-2020-1472
Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

CVE-2020-1472
https://github.com/VoidSec/CVE-2020-1472
Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will resets the Domain Controller's account password to an empty string.

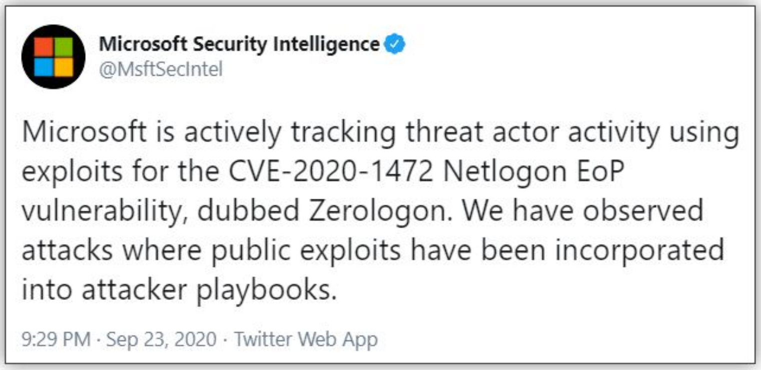
Silverfort's Scanner for Vulnerable DCs with Zerologon
https://github.com/silverfort-open-source/zerologon-entire-domain-tester

https://github.com/rsmudge/ZeroLogon-BOF

Add exploit (aux/admin) for CVE-2020-1472 (AKA: Zerologon)
https://github.com/rapid7/metasploit-framework/pull/14151
This adds an exploit module for CVE-2020-1472, AKA Zerologon. This is a pure-Ruby implementation, leveraging the changes proposed in rapid7/ruby_smb#164.

Next, the DHS/CISA issued an emergency directive requiring all federal agencies to be updated by midnight of the Monday before last Tuesday's podcast.

And finally, the day after that podcast, Microsoft Tweeted:



Microsoft Security Intelligence
@MsftSecIntel

Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon. We have observed attacks where public exploits have been incorporated into attacker playbooks.

9:29 PM · Sep 23, 2020 · Twitter Web App

I note their use of “EoP” for Elevation of Privilege. I suppose that technically the ZeroLogon vulnerability is an elevation of privilege, after you subvert the connection's encryption by using null initialization vectors, bypass the domain controller's authentication, null its password and then logon as the domain admin. Yeah... I'd say that you would have definitely elevated your privileges in this instance.

Or, the sequence as Secura put it:

1. Spoof the client credential
2. Disable RPC Signing and Sealing
3. Spoof a call
4. Change a Computer's AD Password
5. Change the Domain Admin Password

And that all happens in a split second.

Microsoft Security also tweeted three hashes for three files which are known to be used in this exploit. Bleeping Computer tracked those three down to samples that had been uploaded to VirusTotal, all three were named “SharpZeroLogon.exe”:

(45/71 detections)
https://www.virustotal.com/gui/file/b9088bea916e1d2137805edeb0b6a549f876746999fbb1b4890fb66288a59f9d/detection

(42/69 detections)
https://www.virustotal.com/gui/file/24d425448e4a09e1e1f8daf56a1d893791347d029a7ba32ed8c43e88a2d06439/detection

(43/71 detections)
https://www.virustotal.com/gui/file/c4a97815d2167df4bdf9bfb8a9351f4ca9a175c3ef7c36993407c766b57c805b/detection

With detection rates of 45/71, 42/69 & 43/71) the VirusTotal detection rates raised this well above any sort of false-positive, but they still seemed quite low given the severity of the issue today. Wondering whether more A/V might now find it, I had VirusTotal perform a rescan of the original three files. Each of the three files’ detection rates bumped up by 2 or 3, but only to where they are now. I don’t think I’d want to be relying upon any of those A/V tools that was still blissfully unaware of the ZeroLogon threat at this late stage.

Bleeping Computer wrote: “In one of the samples examined by BleepingComputer, and like other public exploits, the NTLM hash of the domain controller will be changed to 31d6cfe0d16ae931b73c59d7e0c089c0, which is the hash for an empty password.”

And now for the SAMBA connection that was just coming to light last week...

It turns out that Samba, the open source implementation of the Server Message Blocks (SMB) protocol for Linux and Unix systems, which maps directory shares between Windows and the “*nixes”, also incorporates the Netlogon protocol, and thus also suffers from the vulnerability.

RedHat had a good write up about this from their perspective:
https://access.redhat.com/articles/5435971

> Red Hat is responding to a vulnerability (CVE-2020-1472) in the Microsoft Netlogon service. Netlogon service is an authentication mechanism used in the Windows Client Authentication Architecture which verifies logon requests, and it registers, authenticates, and locates domain controllers. The netlogon service, as part of the domain controller functionality, implements Microsoft Netlogon Remote Protocol.
>
> The implementation of netlogon protocol contains a flaw that allows an authentication bypass. This was reported and mitigated by Microsoft as CVE-2020-1472. Since the flaw is a protocol level flaw, and Samba implements the protocol, Samba is also vulnerable.
>
> The Microsoft Windows Netlogon Remote Protocol (MS-NRPC) reuses a known, static, zero-value initialization vector (IV) in AES-CFB8 mode. This allows an unauthenticated attacker to impersonate a domain-joined computer, including a domain controller, and potentially obtain domain administrator privileges.
>
> In Windows environments, only the domain controller runs the netlogon service accessible by clients. This applies to Samba when it is used as a domain controller. Samba Domain Controller role is implemented in both Active Directory mode and also the classic/NT4-style mode. The RHEL version of the Samba package only provides classic/NT4-style domain controllers.
>
> An unauthenticated attacker with network access to a domain controller can impersonate any domain-joined computer, including a domain controller. The attack can result in a denial of service and potentially allow an attacker to gain domain administrator privileges.
>
> To protect against the attack described in CVE-2020-1472, an authenticated connection to netlogon service must be used. Such a requirement is known as a secure channel establishment between domain members and domain controllers, commonly referred to as 'schannel'. Schannel setup prevents unauthenticated access to netlogon service and thus mitigates any attack vector described in CVE-2020-1472.
>
> The Samba suite supports secure channel establishment between domain members and domain controllers. However, default behavior for server schannel prior to Samba 4.8 was to automatically negotiate secure channel only if a client supports it. Since version 4.8, the default behaviour of Samba has been to insist on a secure channel for all clients, which is a sufficient fix against the known exploits of CVE-2020-1472 attack. This default is equivalent to having 'server schannel = yes' in the smb.conf.
>
> Requiring a secure channel might break some old applications which originate from pre-Active Directory time (NT4 domains). Due to this, Microsoft's mitigation for CVE-2020-1472 does not immediately disable unauthenticated access to netlogon service. Red Hat is not aware of any specific applications that require use of an unauthenticated channel to netlogon service. All Samba components in all Red Hat Enterprise Linux (RHEL) versions do support operating with schannel established, and will continue to work when future updates from Microsoft will disable unauthenticated channel support altogether.
>
> Default configurations of the samba and samba4 packages shipped with Red Hat Enterprise Linux 6 are vulnerable as they do not enforce secure channel establishment for all client connections to the netlogon service. The vulnerability can be mitigated by following the

> instructions mentioned in the “Mitigation” section.
>
> Default configurations of the samba packages shipped with Red Hat Cluster Storage 3, and Red Hat Enterprise Linux 7 and 8 are not vulnerable by default. They enforce secure channel establishment for all client connections to the netlogon service. If Samba configuration, smb.conf, changed to explicitly state 'server schannel = no' or 'server schannel = auto', such a setup would be vulnerable.
>
> File servers and domain members (using any supported version of samba shipped with Red Hat Enterprise Linux) do not run the netlogin service and only need to ensure that they have not set 'client schannel = no' for continued operation against secured DCs such as Samba 4.8 and later and Windows DCs in 2021.

So, to summarize, since Samba v4.8, which was released in March 2018, the default behaviour of Samba has been to insist on a secure netlogon channel, which is a sufficient fix against the known exploits. This default is equivalent to having 'server schannel = yes' in the smb.conf.

Therefore versions 4.8 and above are **not** vulnerable **unless** they might have been configured not to require a secure channel for netlogon by setting 'server schannel = no' or 'server schannel = auto' in its smb.conf lines.

Samba versions 4.7 and below **are** vulnerable unless they have 'server schannel = yes' in the smb.conf.

And a convenient micropatch (0-patch)
Mitja Kolsec, CEO and co-founder at 0patch, has stepped up with another of their terrific micropatches (this one a whopping 29 bytes). The first two sentences of his blog read:

“The Zerologon vulnerability allows an attacker with network access to a Windows Domain Controller to quickly and reliably take complete control of the Windows domain. As such, it is a perfect vulnerability for any attacker and a nightmare for defenders.”

In an interview with ThreatPost, Mitja explained: “Our micropatch was made for Windows Server 2008 R2, which reached end-of-support this January and stopped receiving Windows updates. Many organizations are still using this server and the only way for it to get extended security updates from Microsoft was to move it into the Azure (cloud) — which is an unacceptable option for most organizations.” He also added that 0patch is also working on porting the micropatch to various still-supported Windows Servers for customers who, for various reasons, can’t apply the Microsoft patch.

His blog provides a truly WONDERFUL look into the micro-patch development process and it is this week's GRC Shortcut URL: https://grc.sc/786 (Or you can also “Duck It” by searching for “0patch ZeroLogon” — and, yes... I did just say “Duck It!”)

https://blog.0patch.com/2020/09/micropatch-for-zerologon-perfect.html

In this blog posting, Mitja explains in detail what's going on, what the patch developers faced, and what they created... and they include the full source code for the micro-patch which eliminates this vulnerability. They essentially duplicated what Microsoft did, but since the target server platform is 2008 R2, the specific function that was patched in later servers is not present. So they had to implement the same patch functionality somewhere else in the authentication flow. And they did.

So...

“The Perfect” vulnerability explodes onto the scene. It’s simple to do. It’s incredibly powerful and destructive if it can be used. It’s every Ransomware villain’s dream come true... and GitHub is filled with sample source code implementations.