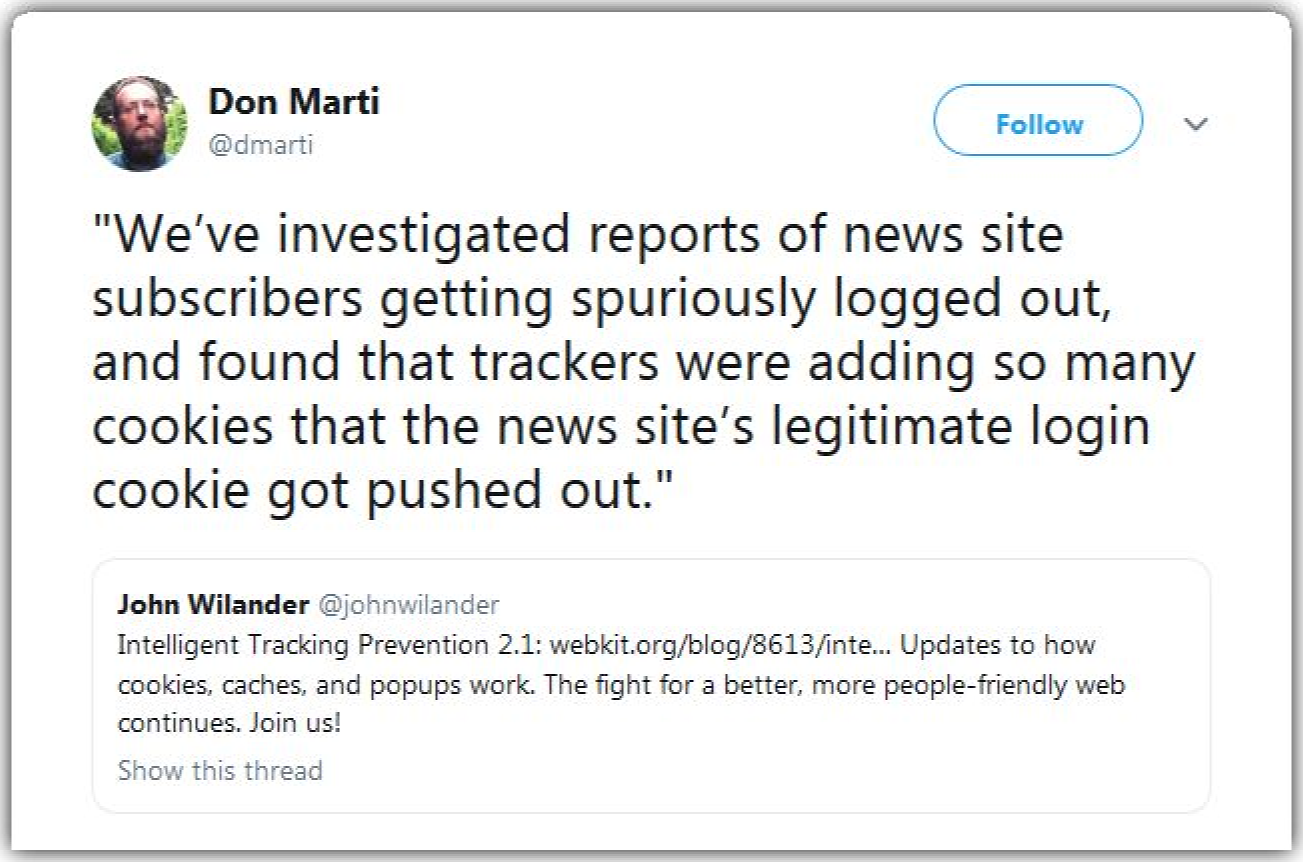
Security Now! #703 - 02-26-19
Out in the Wild

This week on Security Now!

This week we discuss a number of ongoing out-in-the-wild attacks along with a bunch of other news. We have another early-warned Drupal vulnerability that has immediately come under attack in the wild and a 19-year old flaw in an obscure decompress for the "ACE" archive format, which, until a few days ago WinRAR was supporting to its detriment, Microsoft reveals an abuse of HTTP/2 protocol which is DoSing its IIS servers, Mozilla faces a dilemma about a wanna-be Certificate Authority and they also send a worried letter to Australia. Microsoft's Edge browser is revealed to be secretly whitelisting 58 web domains which are allowed to bypass it's "Click-To-Run" permission for FLASH, ICANN renews its plea for the Internet to adopt DNSSEC, NVIDIA releases a handful of critical driver updates for Windows, and Apple increases the intelligence of it's Intelligent Tracking Prevention.

Bringing new meaning to the term ”Cookie Monster”


Don Marti
@dmarti

"We’ve investigated reports of news site subscribers getting spuriously logged out, and found that trackers were adding so many cookies that the news site’s legitimate login cookie got pushed out."

John Wilander @johnwilander
Intelligent Tracking Prevention 2.1: webkit.org/blog/8613/inte... Updates to how cookies, caches, and popups work. The fight for a better, more people-friendly web continues. Join us!

Security News

Another early warning of a forthcoming critical Drupal Security update:

Date: 2019-February-19
Security risk: Highly critical 20/25 AC:None/A:None/CI:All/II:All/E:Theoretical/TD:Uncommon
Vulnerability: Critical Release
Description: There will be a security release of 8.5.x and 8.6.x on February 20th 2019 between 1PM to 5PM America/New York (1800 to 2200 UTC). (To see this in your local timezone, refer to the Drupal Core Calendar) . The risk on this is currently rated at 20/25 (Highly critical) AC:None/A:None/CI:All/II:All/E:Theoretical/TD:Uncommon.

Not all configurations are affected. Reserve time on February 20 during the release window to determine whether your sites are affected and in need of an immediate update. Mitigation information will be included in the advisory.

Contributed module security updates may also be required.

If you are running Drupal 7, no core update is required, but you may need to update contributed modules if you are using an affected module. We are unable to provide the list of those modules at this time.

Neither the Security Team nor any other party is able to release any more information about this vulnerability until the announcement is made. The announcement will be made public at https://www.drupal.org/security over Twitter, and in email for those who have subscribed to our email list. To subscribe to the email list: log in on Drupal.org, go to your user profile page and subscribe to the security newsletter on the Edit » My newsletters tab.

Security release announcements will appear on the Drupal.org security advisory page.

Hopefully, if you are running Drupal v8.5.x or v8.6.x, this is old news to you, because...

Two days after Drupal's disclosure, two different sites published proof-of-concept code,
... And the day after that, using one of those PoC's as its foundation, attacks against Drupal sites began.

Yesterday, Imperva security summed up their observations for the preceding two days:

https://www.imperva.com/blog/latest-drupal-rce-flaw-used-by-cryptocurrency-miners-and-other-attackers/

Edi Kogan: Latest Drupal RCE Flaw Used by Cryptocurrency Miners and Other Attackers

Another remote code execution vulnerability has been revealed in Drupal, the popular open-source Web content management system. One exploit — still working at time of this writing — has been used in dozens of unsuccessful attacks against our customers, with an unknown number of attacks, some likely successful, against other websites.

Published on February 20th, the new vulnerability (known as CVE 2019-6340 and SA-CORE-2019-003) is about field types that don't sanitize data from non-form sources when the Drupal 8 core REST module and another web services module such as JSON:API are both enabled. This allows arbitrary PHP remote code execution that could lead to compromise of the web server.

An exploit was published a day after the vulnerability was published, and continues to work even after following the Drupal team's proposed remediation of disabling all web services modules and banning PUT/PATCH/POST requests to web services resources. Despite the fix, it is still possible to issue a GET request and therefore perform remote code execution as was the case with the other HTTP methods. Fortunately, users of Imperva's Web Application Firewall (WAF) were protected.

https://www.ambionics.io/blog/drupal8-rce
https://paper.seebug.org/821/

Imperva: As always, attacks followed soon after the exploit was published. So being up to date with security updates is a must.

According to Imperva's research, 2018 saw a year-over-year increase in Drupal vulnerabilities with names such as DirtyCOW and Drupalgeddon 1, 2 and 3. These were used in mass attacks that targeted hundreds of thousands of websites.

Imperva noted that there were a few interesting payloads in the most recent attacks. One payload attempts to inject a Javascript cryptocurrency (Monero and Webchain) miner named CoinIMP into an attacked site's index.php file so that site visitors will run the mining script when they browse the site's main page, for the attacker's financial benefit.

The attacker's payload also tries to install a shell uploader to upload arbitrary files on demand.

The guys who developed the PoC code are "Ambionics Security." They wrote the following:

Once again, an RCE vulnerability emerges on Drupal's core. This time it is targeting Drupal 8's REST module, which is present, although disabled, by default. [REST = Representational State Transfer] By making use of the patch provided by Drupal, we were able to build a working exploit; furthermore, we discovered that the immediate remediation proposed for the vulnerability was incomplete, which could lead to a false sense of security. We therefore decided to release our findings, along with an exploit POC.

[Note that, here, again, the fix for a problem inherently exposes the problem's nature. When buggy code is distributed in compiled form it is far more difficult for bad guys, or even misdirected good guys, to examine the patched version to reverse engineer what was fixed. But when the buggy code is inherently distributed as readily readable PHP source, as is the case with any PHP-based system, reverse engineering the problem is a simple matter of running a source code comparison. So it's no great accomplishment that these guys were able to quickly produce and publish a proof of concept.]

Drupal's advisory is fairly clear about the culprit: the REST module, if enabled, allows for arbitrary code execution. Nevertheless, writes Ambionics, Drupal's assertion that PATCH or POST requests must be enabled is wrong. The RCE is triggerable through a GET request without any form of authentication, even if POST/PATCH requests have been disabled in the REST configuration.

Therefore, the recommendation to "not allow PUT/PATCH/POST requests to web services resources" is incorrect, and does not protect from the vulnerability. Upgrading your Drupal, or disabling the REST module is, at the moment, the only solution.

In their disclosure, Ambionics noted: "By diffing Drupal 8.6.9 and 8.6.10..." In other words, they what I assumed and simply looked at the difference between the two PHP source files to see what was changed, then figured out how to exploit the original code.

The repaired versions are v8.5.11 and v8.6.10.

The takeaway for our listeners is, if you are a Drupal site, be absolutely certain that you are receiving Drupal security notices. As Drupal said: To subscribe to the email list: log in on Drupal.org, go to your user profile page and subscribe to the security newsletter on the Edit » My newsletters tab.

Drupal has built a very nice system. But it does suffer from having a large exposed attack surface and being published in PHP source. This means that being on the ball and making the time to keep it current, even when it may be inconvenient to do so, comes with the territory.

The WinRAR "ACE" format RCE

Yesterday, security researchers at the 360 Threat Intelligence Center (360TIC) detected an in-the-wild malspam email campaign that's distributing a malicious RAR archive file that exploits the newly discovered WinRAR vulnerability to install malware on computers running the vulnerable version of the software.

Approximately 500 million users have WinRAR installed on their computers. I'm one of them since the RAR archive format can be tuned to compress significantly better than ZIP, so RAR's have long been my preferred and standard means of maintaining archives for my various systems.

WinRAR is extremely flexible. In addition to RAR's and ZIP's, WinRAR is also able to open and unpack CAB, ARJ, LZH, TAR, GZ, TAR.GZ, BZ2, TAR.BZ2, UUE (remember those?) JAR (Java Archive), ISO (ISO9660 - CD image), 7Z, XZ,Z (Unix compress).

And... Until a few days ago, it was also able to unpack ACE format archives. I don't recall ever encountering an "ACE" format file, so I looked it up on Wikipedia and learned that: "ACE is a proprietary data compression archive file format developed by Marcel Lemke, and later bought by e-merge GmbH. The peak of its popularity was 1999–2001, when it provided slightly better compression rates than RAR, which has since become more popular." The original utility that worked with ACE was adware driven, and proprietary, so one else was able to produce its ACE format. The various archivers were only able to open ACE archives by using the closed-source

UNACE.DLL... And, it turns out, it is in this DLL that a newly discovered and worrisome vulnerability lies:

Security researchers at CheckPoint found a very old (19 year old) problem: They discovered an "Absolute Path Traversal" bug in the library that could be leveraged to execute arbitrary code on a targeted system when attempting to uncompress a maliciously-crafted file archive using vulnerable versions (apparently they were all vulnerable) of the software. The path traversal flaw allows attackers to extract compressed files to a folder of their choice rather than the folder chosen by the user, creating the opportunity to drop malicious code into, for example, the Windows Startup folder where it would automatically run on the next reboot.

Therefore, to take full control of a targeted computer where WinRAR had been installed, all an attacker needs to do is convince the machine's user into opening maliciously crafted compressed archive file.

The WinRAR team no longer has (if they ever did have) the source code of the UNACEV2.dll. They have simply been including its DLL since... Why not? Well, now we have a "why not" so all support for the ACE format has been dropped in the just-released WinRAR version 5.70 beta 2.

Also note that since WinRAR detects the format by the CONTENT of the file and not by the extension, attackers can change the .ace extension to .rar extension to make it look normal friendly.

So... Everyone listening to this podcast who has WinRAR should go get the latest. I did, and pesky ACE support that was there is now gone.

Microsoft's latest web servers are vulnerable to a CPU-saturation attack
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190005

Gal Goldshtein of F5 Networks found and reported a vulnerability affecting Microsoft's recent implementation of the HTTP/2 web protocol. So this affects all IIS servers running Windows Server 2016, Windows Server Version 1709 and 1803, as well as Windows 10 (versions 1607, 1703, 1709, and 1803.)

It turns out that by setting up a maliciously-crafted HTTP/2 connection, it's possible for any remote attacker to trigger an effective DoS condition through an IIS resource exhaustion bug that "could temporarily cause the system CPU usage to spike to 100% until the malicious connections are killed by IIS."

Microsoft wrote: The HTTP/2 specification allows clients to specify any number of SETTINGS frames with any number of SETTINGS parameters. In some situations, excessive settings can cause services to become unstable and may result in a temporary CPU usage spike until the connection timeout is reached and the connection is closed. The default IIS connection timeout is 2 minutes. This makes overlapping connections, triggered at 1-minute intervals trivial to perpetrate in order to hold any IIS server permanently offline.

In their advisory, Microsoft states that there are no known mitigations or workarounds for the vulnerability and it recommends all users to install the February non-security updates listed in the advisory's table.

There are 14 editions of Windows with a total of four patch editions among them, so you'll need to choose the correct one. This really doesn't affect anyone who doesn't have an IIS web server exposed to the public Internet. If you're a Windows 10 user at home or office behind any NAT router, your instance of IIS -- which is probably not even running -- won't be affected.

Who do we trust to be in our certificate root store?

A company named "DarkMatter" based in the UAE (the United Arab Emirates) is petitioning Mozilla to include their CA root in Firefox. The problem is, DarkMatter has been known to sell surveillance and hacking services to oppressive regimes throughout the Middle East and last month a report by Reuters further described DarkMatter's involvement in helping the Saudi government spy on dissidents.

https://www.reuters.com/investigates/special-report/usa-spying-raven/

Project Raven: Inside the UAE’s secret hacking team of American mercenaries
Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy — dissidents, rival leaders and journalists.

I'll tell you right now, I use Firefox and I don't want any CA root cert from a company who chose to name itself "DarkMatter" anywhere near my machine. No thank you. The only possible reason to be carrying such a certificate is if I'm going to be visiting a site whose TLS certificate was purchased from "DarkMatter" -- so that's a chance I'm happy to take.

It's true that certificate mis-signing is difficult to pull off in today's world with the degree of welcome certificate issuance oversight we have in our industry today. But the benefit seems so marginal compared to the risk.

Mozilla is under pressure by the Electronic Frontier Foundation, Amnesty International, and The Intercept to decline DarkMatter's request. But DarkMatter, which DOES have the ability to issue certificates because it is trusted by another well-placed CA, QuoVadis, claims that it has never abused its TLS certificate issuance powers for anything bad... So there's no basis for treating it with less trust than other CAs that have applied in the past. DarkMatter wishes to move from a 2nd class CA up to first class status.

Concerns are further heightened because Mozilla's list of trusted root certificates is also used by some Linux distros. Thus there are fears that once approved and added to Mozilla's certificate store list, DarkMatter would be able to issue TLS certificates to intercept Internet traffic without triggering errors or warnings on Linux systems which are often deployed in data centers and at cloud service providers.

So Mozilla has a dilemma, but many are not the least bit ambivalent:

The EFF's Cooper Quintin said in the Google Groups discussions. "Given DarkMatter's business interest in intercepting TLS communications, adding them to the trusted root list seems like a very bad idea. I would go so far as revoking their intermediate certificate as well, based on these revelations."

Quintin expanded on his fears in a post on the EFF blog, reminding Mozilla that it went through a similar issue 20 years ago in 2009 with CN-NIC, the Chinese government's official CA. Back in 2009 Mozilla approved CN-NIC as a trusted root CA in Firefox, after which (six years later) the CA was caught mis-issuing certificates for Google domains in 2015, thus allowing threat actors to intercept traffic meant for Google sites... which got CN-NIC banned from most certificate root stores.

And the outcry against this CA addition is overwhelming its support. Mozilla publicly posted that "Mozilla's Root Store Policy grants us the discretion to take actions based on the risk to people who use our products. Despite the lack of direct evidence of mis-issuance by DarkMatter, this may be a time when we should use our discretion to act in the interest of individuals who rely on our root store."

Amen.

If necessary give us an option "[ ] Allow Sketchy CAs" and I'll be sure it's turned off in my browser!

Meanwhile, Mozilla worries that its employees could be subject to Australia's legislation...

Sophos' headline which caught my attention and puzzled me was: "Mozilla fears encryption law could turn its employees into insider threats"

Last Friday, February 22nd, Mozilla wrote to the Committee Secretary of the Australian Parliamentary Joint Committee on Intelligence and Security

RE: Comments for Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication & Other Legislation Amendment (Assistance & Access) Act of 2018

Thank you for the opportunity to provide comment as part of your review of Telecommunication & Other Legislation Amendment (Assistance & Access) Act of 2018 (TOLA). This legislation grants sweeping and dangerous new powers to Australian law enforcement and intelligence agencies, and thanks to the foreign assistance provisions, extends these powers to foreign authorities as well. In doing so, this legislation raises grave concerns for the security of internet users and infrastructure in Australia and abroad, and fails to place appropriate limits on government surveillance. Given the serious threats to security and privacy posed by this Act, we welcome the Committee’s review of this legislation and urge you to move swiftly to ameliorate its harms.

Mozilla’s mission is to ensure the internet is a global public resource, open and accessible to all. Our flagship product is Firefox, which is an openly developed and open source web browser used by hundreds of millions of people worldwide. The Firefox code base is also used for the Tor browser, which allows anonymous browsing. In addition to protecting the security of our products, Mozilla has influenced core security protocols used in the internet and backed the adoption of HTTPS, which encrypts website connections to enable more private and secure browsing. In addition, we have advocated to judges and policy makers in many countries on the importance of transparent and robust government processes to handle security vulnerabilities and surveillance requests.

As we noted in our submission to this Committee when this legislation was initially under consideration: “Any measure that allows a government to dictate the design of internet systems represents a significant risk to the security, stability, and trust of those systems. Mozilla believes that TCNs or any similar device would significantly weaken the security of the internet.”

We do not believe that this law should have been passed in the first place, and we believe the best possible path is to repeal this legislation in its entirety and begin afresh with a proper, public consultation.

While it is our absolute preference that this legislation be abandoned and annulled, we recognize that the political will may not exist to take this action to protect the security of all Australians. To that end, in the remainder of our submission, we focus on a series of amendments that could be offered to avoid some of the most dangerous consequences of this law on the security of the internet. In order of priority, we urge the Committee and the Australian Parliament to, at a minimum, make the following changes:

1. Clarify that Australian authorities cannot target an employee of a Designated Communications Provider.

2. Remove restrictions on disclosure of Technical Assistance Requests, Technical Assistance Notices, and Technical Capability Notices.

3. Require judicial approval of Technical Assistance Notices and Technical Capability Notices.

4. Modify the assessments mechanism to ensure an impartial review which considers all rights and interests.

5. Require all requests not to disproportionately harm the rights and interests of users not under suspicion.

6. Clarify that “systemic weakness” includes any weakness in an individual communications system available to more than one person.

7. Limit the delegation of powers in TOLA.

8. 8. Impose critically missing limitations on providing assistance to foreign authorities and extraterritorial use of these powers.

We provide additional detail and recommendations on each of these points below. We look forward to engaging with the Committee as you conduct this critical review of TOLA. If you have any questions about our submission or if we can provide other information that would be helpful to the Committee as part of your review, please contact Mozilla Senior Global Policy Manager Jochai Ben-Avie.

1. Clarify that Australian authorities cannot target an employee of a Designated Communications Provider

Due to ambiguous language in TOLA, one could interpret the law to allow Australian authorities to target employees of a Designated Communications Provider (DCP) rather than serving an order on the DCP itself through its General Counsel or an otherwise designated official for process. It is easy to imagine how Australian authorities could abuse their powers and the penalties of this law to coerce an employee of a DCP to compromise the security of the systems and products they develop or maintain. In order to ensure due process, appropriate diligence, and full compliance where appropriate with orders issued under this legislation, we strongly believe that Australian authorities should only serve an order on the DCP itself. Serving an order on an individual employee rather than a DCP itself would fail to allow a DCP to avail itself fully of the protections afforded under this legislation in regards to consultations, assessments, and legal challenges. Further, this potential would force DCP's to treat Australia-based employees as potential insider threats, introducing another vector for compromise that could undermine trust in critical products and incentivizing companies to move critical roles to other localities. Parliament recognized the wisdom of this limitation in regards to Contracted Service Providers, but not DCPs.

We recommend the Committee: ADD a clarification in the Section 317B definition of Designated Communications Provider to specify that this term "does not include a person who performs such services in their capacity as an employee, agent, or vendor of the provider."

https://www.aph.gov.au/DocumentStore.ashx?id=7609a72e-1452-4a20-b76a-87e55d1243bc&subId=666681

Here's a real headshaker regarding Microsoft Edge and Adobe's ill-fated FLASH plug-in:
Believe it or not, Microsoft's Edge web browser comes with a deliberately hidden and obscured whitelist specifically to allow Facebook to circumvent the request for user consent with its built-in click-to-play security policy for Flash content.

Back on November 26th, Google Project Zero's Ivan Fratric posted: In Microsoft Windows, there is a file C:\Windows\system32\edgehtmlpluginpolicy.bin that contains the default whitelist of domains that can bypass Flash click2play and load Flash content without getting user confirmation in Microsoft Edge.

Today's updated version of the previously secret Edge whitelist only allows Facebook to bypass the Flash click-to-play policy on its www.facebook.com and apps.facebook.com domains.

In his bug report, Ivan also highlighted the security implications of having a Flash autorun whitelist bundled with a web browser, especially given the number of Flash security patches issued by Adobe almost every month.

This whitelist is insecure for a number of reasons. As we mentioned last week, by far the most common and most prevalent problem on today's web are cross-site scripting (XSS) vulnerabilities. With this sort of domain-name-based whitelist, a cross-site scripting vulnerability on any of the whitelisted sites would allow a bypass of the click2play policy. And, moreover, there are currently publicly known and unpatched instances of XSS vulnerabilities on at least some of the whitelisted domains.

Also, the whitelist is not limited to https and limiting FLASH to HTTPS wouldn't work anyway as some of the whitelisted domains don't support https at all! Even in the absence of a cross-site scripting vulnerability, this would allow a MITM attacker to bypass the click2play policy.

As I mentioned above, the big issue reported by Fratric was partially addressed by Microsoft during this month's Patch Tuesday by trimming the whitelist down to just the two Facebook domains, and by adding HTTPS support as a requirement for all the entries on the whitelist to mitigate the possibility of MITM attacks.

However, on Windows 10 v1803 back in November, the whitelist contained the SHA256 hashes for 58 domains which Ivan was able to reverse to obtain this list:

Hash	Cleartext
01d004ae59fe9d0902b0e4526999432118199654f78b0384e4eb983e986d562d	www.pogo.com
0309388894379c1e0d01081f6f4d5d4412a82dc5b9bd66476de2270b361cecfd	www.wasu.cn
0ae9eeba3229fa449ff5fcf42692cad2305e14933a6102187e94c48346ab8c9d	www.tvnow.de
0bc8e61a5970eb325f02148c05b79d60a9a0462efc18a6a60b7f8cd2dc84ccbc	chushou.tv
0bfc80d67c9b57f3f1bb978344c8d8d6ac19786e261f98c1c9735f6ba5ec344c	more2.starfall.com
1136593de37540f6f5396fdbbf93aa070c2b1c844d2d3d06de5373831a9df3bf	loa.gtarcade.com
12055be963e0f2c7786d1283d343afbaac921513a985a21f5f83b6a82b9582e9	nseindia.com
12c3d9b1a0a1f33a7d7ab1b4ccb53c1163210ee527ad5336175eb40ff1fcfe45	N/A
2135e9b55346dd4146bbfae6f0cc896a39688d3287a952f63ae222837e5de152	www.wgt.com
22af4cad3e57873a50693fe36d6385795ae6c56e4d0d759530f263db571a6b2c	netgauge.unitel.ao
2df0e6efc506a72a4c9e91ebebe70cf8252f1ffbd8b483043b1a856b75d13ce9	www.icourses.cn
2f87a652a9d2880a3ad580ec4a91bde3f4d2d32ac8f792d4258518d46330870f	www.la7.it
2f9f879f017ebe4d6f71a0755eee3b08a5f757c0d011112ded94e6b337b3b520	www.dgestilistas.es
348374ff89afe5693015c3d38758c83867c180a8010372a564c8f5eeaf9b5d0b	www.zxxk.com
3c23924f2f71c05d3b484fbaaa6e4ab4319d5bb3f0a002688132aa0f8434fd3b	weathernews.jp
46bdf3a01ab608d1a5e68923532e610ff7725a68d4bb063c96c8dedd4617404a	**bigfarm.goodgamestudios.com**
4740f56f40ed20eddb576ae29fdf0c507dd06681e949bda8be5611eaf3ad9d3d	www.facebook.com
4779eb7f42cc6736ca2b1e52449799705214f2542fa4cf952e741d8dd5efad31	www.deezer.com
4f5db25a3bd2f1abf3dd1a509b2e1a6d81b9ba4428f333454c29d93e794150bc	N/A
515563682e9bfc44b6fed4459149f83ba7f207bf53f6a0208156ac7c46e59d92	yahoo-mbga.jp
51bfa3e340a5ff7dfa37ad7ad409e5a214caadd0f82fc1fef82d38b766c2f088	**ok.ru**
563d53ee90b355ebd7558c2d9f3bee94489d406c565f9ed5741fb59bbc734544	seer.61.com
5b13e0a388860a0f136eefdd36d2f57fb81f46588ca85e7d93a4fd24cf6462f8	empire.goodgamestudios.com
5e7fc524d10f21da23bc43f24de00967094d69d6f4ccda277fff7042024c3ce5	www.friv.com
5f832e1442b497050d79cd18b32de807e4201a3181929ade823112defa6c1079	video.baomihua.com
64e2991629e5e208874400bc1ea0161fb064f1c2397b1cedc3bb282ea3f4ee3b	hiztesti.turktelekom.com.tr
6793b64c0ccc547a01b8b6982318e25ae3dc0b91dfc09366c7f1f1b3a7fa127e	www.scholastic.com
68fc10e638f0bb2e25149d2ef8d3d87cf318bbf2de7c9aa74131d53e926fe79e	www.viz.com

881bcca2199248b7c82ed14cb1dbd6e87ac9ea899d1f9f02d13d29e837487782	**www.dilidili.wang**
89ac7d2d82b6a2ef952e3d627853180fb250167ed56b893647814e8374d4f5cd	games.aarp.org
900da7ee51cf43450699d9cd11e3cf6ba8d2d04d9d836cd359281d7791e328af	www.douyu.com
9adea347b4e793529c9a5e1a35e2aa7c88772b7e2a086d2d24a4f8ccbb20e3ac	rc.qzone.qq.com
9c97a59b30e879d3245139795adea4380f62e4e14149025f12f69eb3b532e518	www.nicovideo.jp
a2cf2fe6a8822459d81d15b1327b5bac601bafc460fafa716bc2dcc21e9ab50e	www.mynet.com
a77de76633b0717c62034512fb5c3fbb50633ad9b5ebef7a8acf180e455a3025	www.hotstar.com
ad973e7d68dd2c1a8e9f04886e34db40021e1e76eff3bbc53e7ab8934688a4ed	www.4399.com
b61f47eb2fc64b2ad7ee4ae780ea0ac1a886b4f02f1ec8da77db13f920b4874b	**www.bilibili.com**
ba33c2367ea9f0c66b5b3f345be68a0287a96ca797654c0bf9b2e584d2809ccb	www.msn.com
ba3bc78ec1f427cba6e22cbd63dae305814ca0f0740c0dbd494f804fcaef671a	zone.msn.com
c2fda282c3b5875eaeb6d27ecf62b995684d5739ba1e4082d265dd28dd98ef70	www.worldsurfleague.com
ca6efef88504373a9406ed9a31b430d6df8bb60ea630ac698b0d7c4dab0faf7a	**www.stupidvideos.com**
d833be74b7f95eb0ac133c5aa06c71b7792b5051b1a369740694e78525a4d872	entitlement.auth.adobe.com
dd0f56a6b1a1f2908f4ff45438ffa5e05679375ed0aade8e3ab36bf4c0bd40f4	video.fc2.com
dd2ab62df5da52e66844171efc4415a087cc1a8c432312d814a62da582f40e2d	**www.ontvtime.ru**
ddf38cb97def571ec55f58d372db15fe6ee01578adc85b1087823d239d758af8	apps.facebook.com
e2f07d2fb0e6beac78d55962dda9ebcedba6c3ba30bf83b0880fae69d29537bf	www.totaljerkface.com
e35635613116ae9266c41348d2f4978f093c2fe75ae91f010ad23c1be31b833c	www.hungamatv.com
e39ce3cd42a88216ff9060e8b136bdc153f52322f259321a5925e629659684f8	edu.glogster.com
e4003a967100eb3a92e9148a51e7cd302e6ca4bcc34566c671378a4b0756ef66	v.pptv.com
e4dcd660eae7eeb1ea42050b6dcb108a9bedf1a66e3791438c6abe1efc907e1b	life.pigg.ameba.jp
e57c8c0083d4ea6fb4b390682d8ad3dffaeda2d37d1c11b9d29418b4a318e1a9	www.panda.tv
e7bce4b54da6dda25cabbe9da2359fe2833c94ec1ce3edd67077a089ed76ef31	www.vudu.com
e9ce06c9a6a05878802f64fac17399cc0a8452c652403445995a90dc9b19401d	www.nseindia.com
ef7f6be560fb99cff749ac35415beeed4aa86f40e10138858289dde1284661c9	music.microsoft.com
f2313491b771d1180f9c4e9cf979820e276a7833859555976dbf4a529cb2189f	en.ikariam.gameforge.com
f4f46a8b3a55ffb3e3784e6743266ed8d7cd2fdd21f494a82e2772fc68590d1b	www.deraktionaer.tv
fcb0eec77983791a7eeb971a2320f38cdbac2ca16cf3f418f83a00a4338eafd4	www.a1.net
fee3af1754656ed83ba706b46c6fa570b020ff79ad84b5adee4882fbf6adaf0e	www.poptropica.com

Today, Microsoft's decision to deliberately obscure the entries in the original 58-domain whitelist, and the decision to keep Facebook's domains whitelisted even after this month's Patch Tuesday, are two questions that only Microsoft can answer. (And Microsoft strongly prefers not to answer such questions.)

Last Tuesday, Ivan tweeted:

The default Flash whitelist in Edge (https://t.co/JxStUIxByE) really surprised me. So many sites for which I'm completely baffled as to why they're there. Like a site of a hairdresser in Spain (https://t.co/50xdJvzksA)?! I wonder how the list was formed. And if MSRC knew about it.
— Ivan Fratric (@ifsecure) February 19, 2019

ICANN (the Internet Corporation for Assigned Names and Numbers) & DNSSEC
Last Friday, ICANN put out a press release calling for full DNSSEC deployment:
https://www.icann.org/news/announcement-2019-02-22-en

ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet...

LOS ANGELES – 22 February 2019 – The Internet Corporation for Assigned Names and Numbers (ICANN) believes that there is an ongoing and significant risk to key parts of the Domain Name System (DNS) infrastructure.

In the context of increasing reports of malicious activity targeting the DNS infrastructure, ICANN is calling for full deployment of the Domain Name System Security Extensions (DNSSEC) across all unsecured domain names. The organization also reaffirms its commitment to engage in collaborative efforts to ensure the security, stability and resiliency of the Internet's global identifier systems.

As one of many entities engaged in the decentralized management of the Internet, ICANN is specifically responsible for coordinating the top-most level of the DNS to ensure its stable and secure operation and universal resolvability.

On 15 February 2019, in response to reports of attacks against key parts of the DNS infrastructure, ICANN offered a checklist of recommended security precautions for members of the domain name industry, registries, registrars, resellers, and related others, to proactively take to protect their systems, their customers' systems and information reachable via the DNS.

Public reports indicate that there is a pattern of multifaceted attacks utilizing different methodologies. Some of the attacks target the DNS, in which unauthorized changes to the delegation structure of domain names are made, replacing the addresses of intended servers with addresses of machines controlled by the attackers. This particular type of attack, which targets the DNS, only works when DNSSEC is not in use. DNSSEC is a technology developed to protect against such changes by digitally 'signing' data to assure its validity. Although DNSSEC cannot solve all forms of attack against the DNS, when it is used, unauthorized modification to DNS information can be detected, and users are blocked from being misdirected.

ICANN has long recognized the importance of DNSSEC and is calling for full deployment of the technology across all domains. Although this will not solve the security problems of the Internet, it aims to assure that Internet users reach their desired online destination by helping to prevent so-called "man in the middle" attacks where a user is unknowingly re-directed to a potentially malicious site. DNSSEC complements other technologies, such as Transport Layer Security (most typically used in HTTPS) that protect the end user/domain communication.

As the coordinator of the top-most level of the DNS, ICANN is in the position to help mitigate and detect DNS-related risks, and to facilitate key discussions together with its partners. The organization believes that all members of the domain name system ecosystem must work together to produce better tools and policies to secure the DNS and other critical operations of the Internet. To facilitate these efforts, ICANN is planning an event for the Internet community to address DNS protection: The first is an open session during the upcoming ICANN64 public meeting on 9-14 March 2019, in Kobe, Japan.

NVIDIA releases patches for their drivers
NVIDIA has released a security update for their GPU display drivers patching eight security issues that could lead to code execution, escalation of privileges, denial of service, or information disclosure on both Windows and Linux machines.

Though exploitation of the patched problems require local system access and are not remotely exploitable, bad guys that had some other means of running code on a machine could take advantage of these problems once they were able to execute code. The CVSS rating system is a 10-point scale with five of the eight vulnerabilities, for the Windows drivers, receiving an 8.8. The Linux drivers have less severe flaws.

CVE-2019-5665 NVIDIA Windows GPU Display driver contains a vulnerability in the 3D vision component in which the stereo service software, when opening a file, does not check for hard links. This behavior may lead to code execution, denial of service or escalation of privileges.

CVE-2019-5666 NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) create context command DDI DxgkDdiCreateContext in which the product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array, which may lead to denial of service or escalation of privileges.

CVE-2019-5667 NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiSetRootPageTable in which the application dereferences a pointer that it expects to be valid, but is NULL, which may lead to code execution, denial of service or escalation of privileges.

CVE-2019-5668 NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiSubmitCommandVirtual in which the application dereferences a pointer that it expects to be valid, but is NULL, which may lead to denial of service or escalation of privileges.

CVE-2019-5669 NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiEscape in which the software uses a sequential operation to read from or write to a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of the buffer, which may lead to denial of service or escalation of privileges.

CVE-2019-5670 NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiEscape in which the software uses a sequential operation to read from or write to a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of the buffer which may lead to denial of service, escalation of privileges, code execution or information disclosure.

https://www.nvidia.com/Download/index.aspx
As stated above, the flaws would allow attackers to destabilize vulnerable machines at the least, and to possibly run commands and code. There's also an information disclosure flaw that allows attackers to determine the degree to which the system's NVIDIA driver is exploitable. And there are also privilege escalation vulnerabilities.

My system's NVIDIA drivers have not been updated since 2016 and nothing new was available. But if your system is using NVIDIA drivers it would be worthwhile to check for and apply updates.

Apple increases the intelligence of their Intelligent Tracking Prevention (ITP) v2.1.
The beta releases of iOS 12.2 and Safari 12.1 on macOS High Sierra and Mojave include an updated version of Intelligent Tracking Prevention (ITP). For purposes of developer communication.

The update's stated goal is to further reduce trackers’ ability to establish user identities across sites.

A Single Set of Cookies Per Site

Previous versions of ITP allowed domains that were classified with tracking capabilities to store partitioned cookies, i.e. additional sets of cookies keyed off of the top site. As of ITP 2.1, partitioned cookies are no longer supported and third-parties classified with cross-site tracking capabilities now have to use the Storage Access API to get any cookie access.

Apple explains:

Verified Partitioned Cache

WebKit implemented partitioned caches more than five years ago. A partitioned cache means cache entries for third-party resources are double-keyed to their origin and the first-party eTLD+1. This prohibits cross-site trackers from using the cache to track users. Even so, our research has shown that trackers, in order to keep their practices alive under ITP, have resorted to partitioned cache abuse. Therefore, we have developed the verified partitioned cache.

When a partitioned cache entry is created for a domain that’s classified by ITP as having cross-site tracking capabilities, the entry gets flagged for verification. After seven days, if there’s a cache hit for such a flagged entry, WebKit will act as if it has never seen this resource and load it again. The new response is then compared to the cached response and if they match in the ways we care about for privacy reasons, the verification flag is cleared and the cache entry is from that point considered legitimate. However, if the new response does not match the cache entry, the old entry is discarded, and a new one is created with the verification flag set, and the verification process starts over.

(The idea behind what Apple called "Partitioned cookies" was to tie a 1st-party cookie which was set from another page's 1st party domain to that origin domain. This would effectively prevent tracking.)

- 3rd-party cookies are blocked.
- Session cookies for domains not visited for 30 days are deleted.
- Cookies set by browser script rather than websites are removed after 7 days.

Cross-site trackers have started using first-party sites' own cookie jars for the purpose of persistent tracking. The first-party storage space is especially troublesome for privacy since all tracker scripts in the first-party context can read and write each other's data. Say social.example writes a user tracking ID as a news.example first-party cookie. Now analytics.example, adnetwork.example, and video.example can leverage or cross pollinate that user tracking ID through their scripts on news.example.

Cookies available in document.cookie can be stolen by speculative execution attacks on memory. Therefore, they should not carry sensitive information such as credentials.

Cookies available in document.cookie can be stolen by cross-site scripting attacks. Again, therefore, they should not carry sensitive information such as credentials.

The proliferation of cookies slows down page and resource loads since cookies are added to every applicable HTTP request. Additionally, many cookies have high entropy values which means they cannot be compressed efficiently. We come across sites with kilobytes of cookies sent in every resource request.

There is a size limit on outgoing cookie headers for performance reasons, and websites risk hitting this limit when cross-site trackers add first-party cookies. We've investigated reports of news site subscribers getting spuriously logged out, and found that trackers were adding so many cookies that the news site's legitimate login cookie got pushed out.

SQRL:

Van Zeck: Subject: Wow! The magic is real (and in my hands)

Steve,
I just used Jeff's iOS client to login to the SQRL Forums for the first time. As I posted in Jeff's area ... Fantastic! I have read about and watched others use the magic, but it was a real rush to have the magic right in my own hands. Thanks for persevering with SQRL and showing how it is possible to potentially eliminate the biggest hassle (and risk) in internet life -- passwords. I have been lurking around SQRL for all five years, and it is truly exciting to see things come to fruition.
Van

~30~