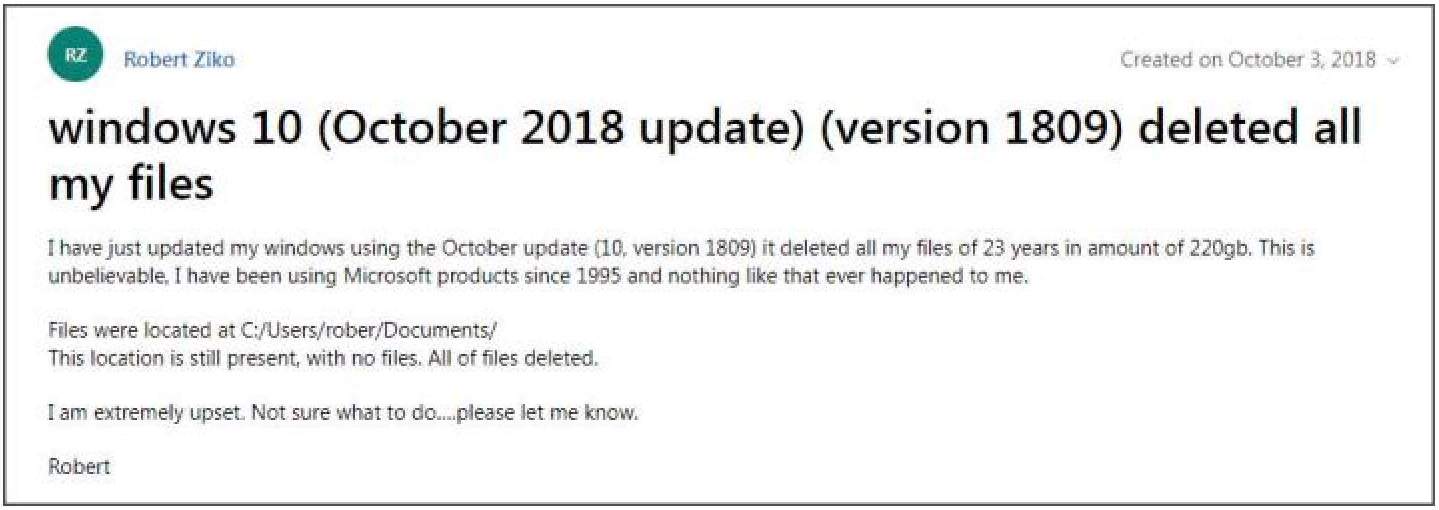
Security Now! #684 - 10-09-18
The Supply Chain

This week on Security Now!

This week we examine and explore an October Surprise of a different sort, a security researcher has massively weaponzied the existing MicroTik vulnerability and released it as a proof-of-concept, a clever voicemail WhatsApp OTP bypass, what happened with that recent Google+ breach?, Google tightens up its Chrome extensions security policies, WiFi radio protocol designations finally switch to simple version numbering, Intel unwraps its 9th-generation Core processors, head-spinning PDF updates from Adobe and Foxit (this isn't a competition, guys!)... and a look at the danger of Supply Chain Attacks, with a possible real world example

An October Surprise



RZ Robert Ziko

Created on October 3, 2018

windows 10 (October 2018 update) (version 1809) deleted all my files

I have just updated my windows using the October update (10, version 1809) it deleted all my files of 23 years in amount of 220gb. This is unbelievable, I have been using Microsoft products since 1995 and nothing like that ever happened to me.

Files were located at C:/Users/rober/Documents/
This location is still present, with no files. All of files deleted.

I am extremely upset. Not sure what to do....please let me know.

Robert

Our Picture of the Week:

On October 3rd, Robert Zeko, under the title "Windows 10 (October 2018 update - version 1809) deleted all my files", posted: I have just updated my Windows using the October update (version 1809) it deleted all my files of 23 years in amount of 220gb. This is unbelievable. I have been using Microsoft products since 1995 and nothing like that ever happened to me.

Files were located at: C:\Users\rober\Documents
This location is still present, with no files. All of the files deleted.
I am extremely upset. Not sure what to do....please let me know.

Security News

The October Surprise: Windows 10 October Update hits a snag...

Last week the pre-release big Windows 10 October feature update was previewed. Fortunately, it had not yet been automatically pushed out to the throngs of waiting Win10 users, though it was publicly available to anyone who wanted to obtain it. Many immediately regretting having done so... because the October update brought many problems.

Microsoft's description page for this update describes it in glowing terms:
https://support.microsoft.com/en-au/help/4464619/windows-10-update-history
“With the release of the Windows 10 October 2018 Update, version 1809, we’re empowering a new era of personal productivity.”

Unfortunately, some who updated, presumably in anticipation of being empowered by this new era of personal productivity, soon discovered that all of their personal documents had been irretrievably deleted from the computer. Seriously. And that was only one of its many problems.

That problem, the most devastating, has not yet been fully articulated. But it was apparently caused by some mess-up with Windows cloud sync. When syncing was not in use, ALL of the user's personal documents would sometimes be irretrievably deleted. As we know, deleted files are not immediately irretrievably lost. Their directory entry is removed, and the physical space they occupied is marked as now available for reuse. So at least some recovery was possible, subject to file fragmentation. Microsoft support was initially caught flat-footed and told people "they'd look into it." Once the problem was better understood the use of file recovery tools -- and the advice to please not use your computer until we get back to you -- was recommended.

Using System Restore to roll back to the pre-October Surprise version could fix Windows itself, but, as we know, system restore doesn't archive non-system personal documents.

Further down that "new era of personal productivity" page, under "Known issues updating to Windows 10, version 1809" Microsoft later added:

> Symptom:
>
> We have paused the rollout of the Windows 10 October 2018 Update (version 1809)* for all users as we investigate isolated reports of users missing some files after updating.
>
> Workaround:
>
> If you have manually checked for updates and believe you have an issue with missing files after an update, please minimize your use of the affected device and contact us directly at +1-800-MICROSOFT, or find a local number in your area.
>
> Alternatively, use a different device to contact us (link will vary according to country of origin). If you have manually downloaded the Windows 10 October 2018 Update installation media, please don’t install it and wait until new media is available.
>
> We will provide an update when we resume rolling out the Windows 10 October 2018 Update to customers.

The good news is, whatever went wrong with the update, not everyone was empowered by the same new era of personal productivity since the full rollout of the now-withdrawn October features was not scheduled to go live until today (Patch Tuesday). So many many more were spared this potential catastrophe.

In addition to the loss of everything in the user's "Documents" folder:

- Task Manager shows incorrect CPU usage levels
- Microsoft Word (at least 2016 and 2019) will no longer Save documents.
- And a number of games including Battlefield 1, Battlefield 4, Assassins Creed, Hitman, Watch Dog and Rainbow Siege reportedly stopped working for some people.

Having observed this, I am =definitely= setting Windows Update on my Win10 machines to wait 60 days before offering feature updates. Unfortunately, Microsoft decided to remove this option from Windows 10 Home machines. So, whatever you do, do NOT manually check for updates.

New Exploit for MikroTik Router WinBox Vulnerability Gives Full Root Access

Let's begin by recalling that MicroTik routers which didn't apply a patch which was made available back in April of 2018 have been vulnerable to a publicly and widely known information disclosure attack. Back then, Mikrotik's patch for this privately reported bug was reverse engineered and turned into a working exploit.

Not only did this MicroTik bug allow remote unauthenticated reading of any file in the router, but the router's username and password database file stored everything in plaintext. In this day and age, that's really unconscionable.

The result, as we have reported, was that massive upsurge of web-based cryptojacking in Brazil. Once some bad guys had obtained the admin login credentials, they used the remote admin interface to replace a file called error.html, transmitted by Mikrotik's built-in web proxy whenever there's an HTTP error, with a web page that loads the CoinHive browser-based cryptomining software. And, as we know, many hundreds of thousands of still-unpatched MicroTik routers are now host to the very nasty VPNFilter malware which Cisco's Talos group spent the summer researching.

So that's a bit of history. Here's what's new...

Near the end of August, MicroTik's security blog posted the following notice:
https://blog.mikrotik.com/security/security-issues-discovered-by-tenable.html

"Security issues discovered by Tenable"
MikroTik was contacted by Tenable Inc. who had discovered several issues in RouterOS web server. The issues only affect authenticated users, meaning, to exploit them, there must be a known username and password on the device. Your data, access to the system and configuration are not under risk. All the below issues only allow the authenticated user (even a read-only user) to cause the www service to crash. Tenable has assigned CVE numbers to these issues.

- CVE-2018-1156: An authenticated user can trigger a stack buffer overflow.
- CVE-2018-1157: File upload memory exhaustion. An authenticated user can cause the www binary to consume all memory.
- CVE-2018-1158: Recursive JSON parsing stack exhaustion, which could allow an authenticated user to cause crash of the www service.
- CVE-2018-1159: www memory corruption, if connections are initiated and not properly cleaned up then a heap corruption occurs in www.

All of the above issues are fixed in the following RouterOS releases: 6.42.7, 6.40.9, 6.43

So these were four potentially serious problems which MicroTik was careful to remind us and keep reiterating were only available to an authenticated user. That's good. However, in their disclosure, MicroTik failed to be explicit about the fact that one of those bugs allowed an attacker to run any program of their choosing, just by making a web request to the router.

But, again, the attacker needed to be authenticated.

But wait... that previous bug which allowed an unauthenticated remote attacked to obtain the router's authenticated account username and password file... would allow an unauthenticated attacker to become authenticated... at which point they could leverage one of these latest authenticated attacks to completely compromise and commandeer any "doubly unpatched" MicroTik router.

And that, ladies and gentlemen, is exactly what has just erupted onto the Internet.

Researchers at Tenable have posted their Proof Of Concept for this on Github under the name "By the Way" they describe it thus:
https://github.com/tenable/routeros/tree/master/poc/bytheway

> "By the Way" is an exploit that enables a root shell on Mikrotik devices running RouterOS versions:
>
> Longterm: 6.30.1 - 6.40.7
> Stable: 6.29 - 6.42
> Beta: 6.29rc1 - 6.43rc3
>
> The exploit leverages the path traversal vulnerability CVE-2018-14847 to extract the admin password and create an "option" package to enable the developer backdoor. Using the then enabled root user "devel" with the admin password, an attacker can then connect to Telnet or SSH with full root remote access.

Anyone can make a mistake. But MicroTik is responsible for its design policies. And the policy of requiring a sophisticated understanding of remote access security from an unsophisticated purchaser of a $49 retail plastic box for the home is simply wrong.

MicroTik has earned and deserves the reputation damage it is suffering within the security community.

Attackers use voicemail hack to steal WhatsApp accounts

A wave of reports about hijacked WhatsApp accounts in Israel induced the Israeli government's cyber-security agency to send a nation-wide security alert last Tuesday. The alert, authored by the Israel National Cyber Security Authority, warns of an effective method of hijacking WhatsApp accounts using mobile providers' voicemail systems.

It's clever and tricky, but it's been know of, in theory for some time, having first been noted a year ago by an Israeli web developer at Oath... and we talked about it here at the time.

The underlying realization was that WhatsApp users who have voicemail accounts for their phone numbers are at risk if they don't change that account's default password, which in most cases defaults to 0000 or 1234.

The opportunity for an account takeover occurs when an attacker tries to add a legitimate user's phone number to a new WhatsApp app installation on his own phone. In that event the WhatsApp service sends a one-time code via SMS to the phone number being joined. This would typically alert a user that something fishy was up... but a hacker could avoid their target becoming aware of this by timing their attack during nighttime or when they are sure the user is away from their phone.

After several failed attempts to validate the one-time code sent via SMS, the WhatsApp service then prompts the user to perform a "voice verification," for which the WhatsApp service calls the user's phone and speaks the one-time verification code verbally. If the attacker has timed their attack properly so that the user doesn't answer their phone, that voice verification message would wind up in the target's voicemail.

And, since most mobile telco providers allow remote access to any customer's voicemail account, all the hacker has to do is to enter the victim's correct voicemail PIN, recover the spoken one-time code, and enter it inside his version of the WhatsApp app. This links the real user's phone number with the hacker's device, and effectively hijacks the account from the legitimate owner.

Once the hacker has gained access to the WhatsApp account, they can then enable two-step verification to prevent the legitimate owner from re-taking control of his WhatsApp account without the 6-digit OTP which only the attacker knows.

The reporting of this has noted that the technique requires minimal technical skills and no specialized equipment. And according to Israeli authorities it has been used widely in recent weeks leading to many reports of hijacked accounts.

In their alert, Israeli authorities recommend that users either use a strong password for their mobile voicemail account or themselves enable two-step verification for the WhatsApp account to prevent the attacker from hijacking the phone number. And note that there is nothing "Israeli-centric" about this. All WhatsApp users everywhere who fit the target profile might also be vulnerable.

Did Google hide a "major" Google+ security flaw that exposed users' personal information?

"Google hid major Google+ security flaw that exposed users' personal information"
"Google+ Shutting Down After Bug Leaks Info of 500k Accounts"
"Google to shut down Google+ after failing to disclose user data breach"
"Google Is Shutting Down Google+ After A Secret Potential Data Leak."
"Google+ to shut down after coverup of data-exposing bug"

Once again, in my opinion, sensationalized breathless headlines get it wrong. Given what Google's own security research auditors found, and given all of the deliberately privacy constrained information Google had at their disposal, I think they have acted responsibly and appropriately.

Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+ https://www.blog.google/technology/safety-security/project-strobe/

I have pulled the relevant bits from their "Project Strobe" posting...

> At the beginning of this year, we started an effort called Project Strobe—a root-and-branch review of third-party developer access to Google account and Android device data and of our philosophy around apps' data access. This project looked at the operation of our privacy controls, platforms where users were not engaging with our APIs because of concerns around data privacy, areas where developers may have been granted overly broad access, and other areas in which our policies should be tightened.
>
> Our review showed that our Google+ APIs, and the associated controls for consumers, are challenging to develop and maintain. Underlining this, as part of our Project Strobe audit, we discovered a bug in one of the Google+ People APIs:
>
> - Users can grant access to their Profile data, and the public Profile information of their friends, to Google+ apps, via the API.
>
> - The bug meant that apps also had access to Profile fields that were shared with the user, but **not** marked as public.
>
> - This data is limited to static, optional Google+ Profile fields including name, email address, occupation, gender and age. Full list:
>
>   https://developers.google.com/+/web/api/rest/latest/people
>
> - It does not include any other data you may have posted or connected to Google+ or any other service, like Google+ posts, messages, Google account data, phone numbers or G Suite content.
>
> - We discovered and immediately patched this bug in March 2018. We believe it occurred after launch as a result of the API's interaction with a subsequent Google+ code change.

> - We made Google+ with privacy in mind and therefore keep this API's log data for only two weeks. That means we cannot confirm which users were impacted by this bug. However, we ran a detailed analysis over the two weeks prior to patching the bug, and from that analysis, the Profiles of up to 500,000 Google+ accounts were potentially affected. Our analysis showed that up to 438 applications may have used this API.
>
> - We found no evidence that any developer was aware of this bug, or abusing the API, and we found no evidence that any Profile data was misused.

On the other hand, since they were deliberately deleting their logs to protect their user's privacy, they would not have evidence of possible historical misuse if there had been any. And frankly, the full list contains a LOT more than just name and eMail address, occupation, gender and age. For example, there's also their birthday, their profile photo, their relationship status, the current and previous employers with dates, the places lived and their skills.

If we assume that they are stating exactly what happened, they are saying that at the time of its patching, 438 applications had access to this API, and that this API could have been misused to leak personal data which was not explicitly marked public. And that as many as 500,000 Google+ accounts were accessible to this privacy-compromising buggy API.

Google explains that they didn't disclose the problem at the time because they had no evidence that any other users of that API were aware of and leveraged that bug during the approximately three years (since 2015) that it was apparently present.

Was Google wrong?

Google Announces Significant Security Updates for Chrome Extensions

As we know and have been discussing a lot, recently, web browser extensions are both an important part of today's web browser ecosystem and, by being powerful, also a significant vector of malicious abuse. Consequently, as we've discussed, earlier this year Google began blocking extensions using cryptocurrency mining scripts. And on June 12th, Google announced their timeline for the deprecation of inline Chrome extension installation:

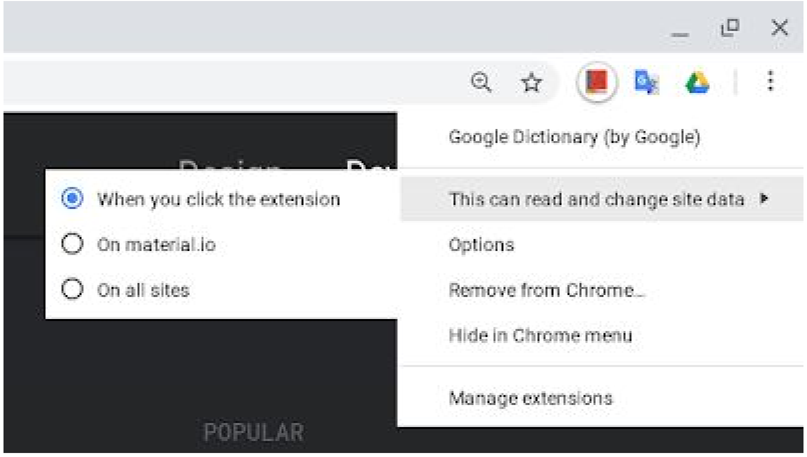
- Starting today, inline installation will be unavailable to all newly published extensions. Extensions first published on June 12, 2018 or later that attempt to call the chrome.webstore.install() function will automatically redirect the user to the Chrome Web Store in a new tab to complete the installation.

- Starting September 12, 2018, inline installation will be disabled for existing extensions, and users will be automatically redirected to the Chrome Web Store to complete the installation.

- In early December 2018, the inline install API method will be removed from Chrome 71.

And now, last Monday, in their posting titled "Trustworthy Chrome Extensions, by Default" Google announced the next set of additional steps they have planned for Chrome 70:
https://security.googleblog.com/2018/10/trustworthy-chrome-extensions-by-default.html

User control over host permissions:
Beginning in Chrome 70, users will have the choice to restrict an extension's host access to a custom list of sites, or to configure extensions to require a click to gain access to the current page:



● When you click the extension
○ On material.io
○ On all sites

Our aim is to improve user transparency and control over when extensions are able to access site data. In subsequent milestones, we'll continue to optimize the user experience toward this goal while improving usability.

Changes to the extensions review process
Going forward, extensions that request powerful permissions will be subject to additional compliance review. We're also looking very closely at extensions that use remotely hosted code, with ongoing monitoring. Extension permissions should be as narrowly-scoped as possible, and all code should be included directly in the extension package, to minimize review time.

New code reliability requirements
Starting today, Chrome Web Store will no longer allow extensions with obfuscated code. This includes code within the extension package as well as any external code or resource fetched from the web. This policy applies immediately to all new extension submissions. Existing extensions with obfuscated code can continue to submit updates over the next 90 days, but will be removed from the Chrome Web Store in early January if not compliant.

Today over 70% of malicious and policy violating extensions that we block from Chrome Web Store contain obfuscated code. At the same time, because obfuscation is mainly used to conceal code functionality, it adds a great deal of complexity to our review process. This is no longer acceptable given the aforementioned review process changes. Additionally, since JavaScript code is always running locally on the user's machine, obfuscation is insufficient to protect proprietary code from a truly motivated reverse engineer. Obfuscation techniques also come with hefty performance costs such as slower execution and increased file and memory footprints. Ordinary minification, on the other hand, typically speeds up code execution as it reduces code size, and is much more straightforward to review. Thus, minification will still be allowed, including the following techniques:

- Removal of whitespace, newlines, code comments, and block delimiters
- Shortening of variable and function names
- Collapsing the number of JavaScript files

Extensions in the store with obfuscated code must be updated using the recommended minification techniques for Google Developers and submitted before January 1st, 2019.

Required 2-step verification
In 2019, enrollment in 2-Step Verification will be required for Chrome Web Store developer accounts. Popular extensions can attract attackers who want to steal it by hijacking developer accounts and 2-Step Verification adds an extra layer of security by requiring a second authentication step via phone or a physical security key. Google strongly recommends enrollment as soon as possible. And it will be required in 2019.

For even stronger account security, consider the Advanced Protection Program. Advanced protection offers the same level of security that Google relies on for its own employees, requiring a physical security key to provide the strongest defense against phishing attacks.

Wi-Fi Gets Simplified Version Numbers and Next Version is Wi-Fi 6
https://thehackernews.com/2018/10/wifi-version-6.html

What's the latest version of Wi-Fi?   It is — Wi-Fi is 802.11ac.

But answering this can be tricky because the underlying Wi-Fi radio technology has not, until now, had a traditional format of version numbering.

The Wi-Fi Alliance—the group that manages the implementation of Wi-Fi—has announced that the next version of WiFi standard, which is 802.11ax, will, instead, use a simpler naming scheme and will simply be called WiFi 6.

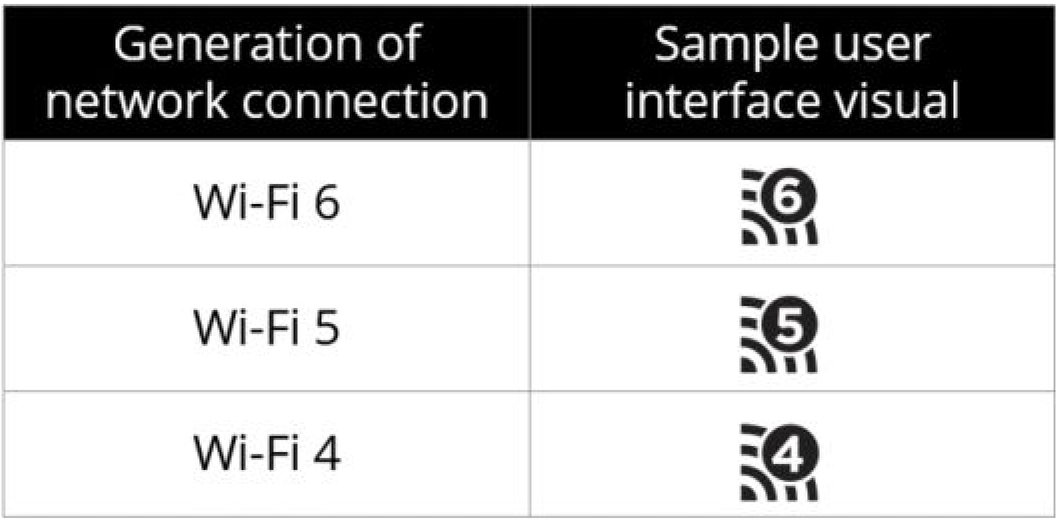
Wi-Fi 6, based on the IEEE 802.11ax standard, will offer higher data rates, increased capacity, better performance even in dense environments (such as stadiums or public venues) and improved power efficiency, making it a worthwhile upgrade for smart home and IoT.

And, earlier versions of the 802.11 wireless standard will get back-ported version numbers:

- 802.11b → Wi-Fi 1
- 802.11a → Wi-Fi 2
- 802.11g → Wi-Fi 3
- 802.11n → Wi-Fi 4,
- 802.11ac (current) → Wi-Fi 5

The WiFi Alliance wrote: "To help users identify devices that provide the latest Wi-Fi experience, Wi-Fi Alliance has introduced simplified generational names that may appear in device names and product descriptions. Wi-Fi devices supporting the latest generation of connectivity are based on the 802.11ax standard and are known as Wi-Fi 6 devices."

The Wi-Fi Alliance also expects manufacturers, operators and software developers to adopt these simple numerical indicators into their user interfaces, instead of classic lettered versions, as shown in the example...



Generation of network connection	Sample user interface visual
Wi-Fi 6	6
Wi-Fi 5	5
Wi-Fi 4	4

Yesterday, Intel unwaped their 9th-Generation Core Processors…
With improvements for the Spectre and Meltdown side-channel attack mitigations built in.

The LGA1151 format CPUs are:

- Intel Core i9-9900K (8 cores, 16 threads, 3.6GHz / 5.0GHz, 95W TDP)
- Intel Core i7-9700K (6 cores, 12 threads, 3.6GHz / 4.9GHz, , 95W TDP)
- Intel Core i5-9600K (6 cores, 6 threads, 3.7GHz / 4.6GHz Turbo, 95W TDP)
- Intel Core i5-9600 (6 cores, 6 threads, 3.1GHz / 4.3GHz Turbo, 65W TDP)
- Intel Core i5-9500 (6 cores, 6 threads, 3.0GHz / 4.1GHz Turbo, 65W TDP)
- Intel Core i5-9400 (6 cores, 6 threads, 2.9GHz / 4.1GHz Turbo, 65W TDP)
- Intel Core i3-9100 (4 cores, 4 threads, 3.7GHz, 65W TDP)
- Intel Core i3-9000 (4 cores, 4 threads, 3.7GHz, 65W TDP)
- Intel Core i3-9000T (4 cores, 4 threads, 3.2GHz, 35W TDP)

One of the slides shown during the presentation contained the text:

> The new desktop processors include protections for the security vulnerabilities commonly referred to as "Spectre", "Meltdown" and "L1TF". These protections include a combination of the hardware design changes we announced earlier this year as well as software and microcode updates.
>
> - Speculative side channel variant Spectre V2 (Branch Target Injection) = Microcode + Software
> - Speculative side channel variant Meltdown V3 (Rogue Data Cache Load) = Hardware
> - Speculative side channel variant Meltdown V3a (Rogue System Register Read) = Microcode
> - Speculative side channel variant V4 (Speculative Store Bypass) = Microcode + Software
> - Speculative side channel variant L1 Terminal Fault = Hardware

So… with the release of the 9th gen CPUs, hardware protection for the L1 Terminal Fault and Meltdown V3 vulnerabilities has been added into the hardware, but mitigations for the other vulnerabilities will still require software and microcode protection… though, of course, in this case the microcode support required will have already been built into the shipping chips.

If you are using Adobe Reader, patch it now!

Last Tuesday, Adobe released security updates for Windows and Mac version of Acrobat and Reader. These updates fix 47 CRITICAL vulnerabilities and 39 that are merely important.

Of the 47 CRITICAL vulnerabilities, 46 allow for code execution and 1 allows for escalation of privileges whereas the 39 “important” vulnerabilities allow for information disclosure.

And, not to be outdone, FoxIt needs to be updated, too!

Foxit recommends all users of Foxit PDF Reader or PhantomPDF to upgrade to version 9.3.

Why?

Foxit’s recent update fixes 116 vulnerabilities, with 18 of them discovered by the Cisco’s Talos group. ALL of the 18 vulnerabilities found by Cisco Talos, as well as many others fixed by this update, are labeled CRITICAL because they could lead to code execution by allowing attackers to create specially crafted web pages or PDFs that could exploit these vulnerabilities to execute commands or install malware on vulnerable computers. And of the 18 vulnerabilities disclosed by Cisco, 12 of them could be exploited simply by visiting a website when the Foxit PDF browser plugin is enabled.

SpinRite

Mark Taylor in Wausaukee, Wisconsin
Subject: Spinrite and encrypted drives
Date: 08 Oct 2018 08:09:33
:
Steve,

All the normal accolades!

Can Spinrite be used on encrypted drives without making the drive unusable because of moved sectors that were fixed?

Thanks Mark

The Supply Chain

Bloomberg: "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies"
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Chinese Spying Chips Found Hidden On Servers Used By US Companies
https://thehackernews.com/2018/10/china-spying-server-chips.html

Chinese spies reportedly inserted microchips into servers used by Apple, Amazon, and others
https://www.theverge.com/2018/10/4/17935868/chinese-spies-microchip-hack-servers-apple-amazon-supermicro

SEE THIS PAGE!! ...

Making sense of the Supermicro motherboard attack | Light Blue Touchpaper
https://www.lightbluetouchpaper.org/2018/10/05/making-sense-of-the-supermicro-motherboard-attack/