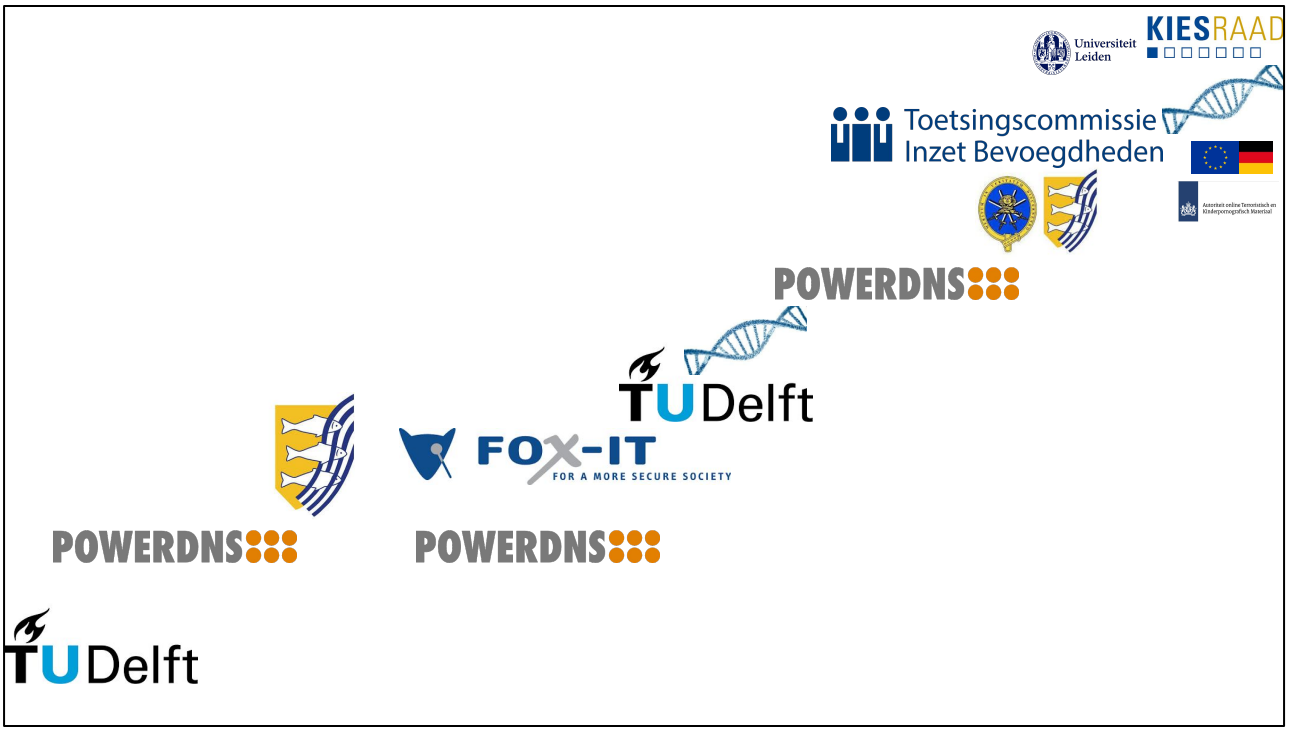
The terrible state of cyber security

A reality check

Bert Hubert
bert@hubertnet.nl

https://berthub.eu/amsec7



Things I have done - only interesting to put my (strong) claims on later pages in context. I failed in my studies of physics, launched an unsuccessful startup (PowerDNS), and when that did not go well joined Dutch intelligence & security agency AIVD. From there I went on to develop software for police and intelligence agencies, while PowerDNS went on. After Fox-IT I did DNA research in Delft again, and then focused on PowerDNS again. After that, I became a regulator of Dutch intelligence services for 2 years. During this time I managed to get my DNA paper published in Nat. Scientific Data.
https://www.nature.com/articles/s41597-022-01179-8

Ik sta hier op eigen titel

Ik spreek namens niemand anders

De toetsingscommissie inzet bevoegdheden opereereert als een soort mini-rechtbank, met ook twee (voormalige) rechters als leden. Was voor mij een geweldige ervaring om in een geheel nieuwe wereld terecht te komen, vol nieuwe gebruiken. Als techneut is het ook leuk om dingen met wetten te doen. Zijn ook stelsels van regels, maar toch werken ze heel anders.

So, where are we?

WORLD NEWS

Dutch government blames a ‘state actor’ for hacking a police network

Updated 1:08 PM GMT+2, October 3, 2024

Share

THE HAGUE, Netherlands (AP) — A cyberattack that broke into a police account and accessed work-related contact details of all Dutch police officers was almost certainly carried out by hackers working for a foreign government, the justice minister told lawmakers.

Dutch intelligence agencies “consider it highly likely that a state actor is responsible,” Justice and Security Minister David van Weel wrote in a letter to lawmakers on Wednesday night about the breach, which was first revealed last Friday.

He added that “police, together with national security partners, are doing everything they can to protect police employees and prevent further damage.”

State of the art setup. Discovered by AIVD.

Office of Personnel Management data breach

From Wikipedia, the free encyclopedia

The **Office of Personnel Management data breach** was a 2015 data breach targeting Standard Form 86 (SF-86) U.S. government security clearance records retained by the United States Office of Personnel Management (OPM). One of the largest breaches of government data in U.S. history, the attack was carried out by an advanced persistent threat based in China, widely believed to be the Jiangsu State Security Department, a subsidiary of the Government of China's Ministry of State Security spy agency.

In June 2015, OPM announced that it had been the target of a data breach targeting personnel records.[1] Approximately 22.1 million records were affected, including records related to government employees, other people who had undergone background checks, and their friends and family.[2][3] One of the largest breaches of government data in U.S. history,[1] information that was obtained and exfiltrated in the breach[4] included personally identifiable information such as Social Security numbers,[5] as well as names, dates and places of birth, and addresses.[6] State-sponsored hackers working on behalf of the Chinese government carried out the attack.[4][7]

Standard Form 86
Revised November 2016
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

Section 21D - Psychological and Emotional Health - *(Continued)*

Complete the following if you responded **'Yes'** to having EVER been diagnosed by a physician or other health professional.

Entry #3

Identify the diagnosis or health condition.

Provide the dates of diagnosis.
From Date *(Month/Year)* ☐ Est. To Date *(Month/Year)* ☐ Present ☐ Est.

Provide the name of the health care professional who diagnosed you, or is currently treating you for such diagnosis, or with whom you have discussed such condition.

Provide the telephone number of the health care professional.
Telephone number Extension ☐ Day ☐ Night ☐ International or DSN phone number

Provide the address of the health care professional who diagnosed you, or is currently treating you for such diagnosis, or with whom you have discussed such condition. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)*
Street City State Zip Code Country

Provide the name of any agency/organization/facility where counseling/treatment was provided. ☐ Same as above

Provide the telephone number of the agency/organization/facility. ☐ Same as above
Telephone number Extension ☐ Day ☐ Night ☐ International or DSN phone number

Provide the address of agency/organization/facility where counseling/treatment was provided. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)* ☐ Same as above
Street City State Zip Code Country

Was the counseling/treatment effective in managing your symptoms?
☐ YES ☐ NO If no, provide explanation ▸

China hacked major U.S. telecom firms in apparent counterspy operation

AT&T, Verizon and Lumen are among the companies breached by Chinese hackers in a sophisticated intrusion by the group dubbed Salt Typhoon, officials say.

6 min 115

U.S. and Chinese flags in Beijing in 2018. (Andy Wong/AP)

One apparent target is information relating to lawful federal **requests for wiretaps**, according to U.S. officials. “There is some indication [the lawful intercept system] was targeted,” the security official said. But the hackers’ access was broader and may have included more general internet traffic coursing through the providers’ systems, they said.

Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history’

The severity of the Chinese breach highlights the need for more telecommunications regulation, lawmakers say.

7 min 680

Senate Intelligence Committee chairman Sen. Mark R. Warner (D-Virginia) and Sen. Marco Rubio (R-Florida) at a hearing on worldwide threats on March 8, 2023. (Drew Angerer/Getty Images)

MOST R

1 Bill indi bril

2 With Trum feder

3 U.S. Willia he w

https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/ – de Chinezen zitten in de tapfaciliteiten van de US telecombedrijven

Tekortkomingen in beveiliging van aftapvoorziening KPN

Nieuwsbericht | 30-08-2022 | 12:00

Agentschap Telecom heeft diepgaand onderzoek gedaan naar de veiligheid van het aftapsysteem van KPN. Hieruit blijkt dat de beveiliging niet op alle onderdelen aan de wettelijke vereisten voldeed. Agentschap Telecom legt daarom een boete op aan KPN van 450.000 euro. KPN geeft aan dat zij de geconstateerde tekortkomingen inmiddels heeft verholpen.

Het onderzoek laat echter ook zien dat een beperkte groep systeembeheerders die toegang had tot de systemen, niet over de vereiste Verklaring omtrent het Gedrag (VOG) en een geheimhoudingsverklaring beschikte. **Deze personen hadden bovendien geen persoonlijk account. Daardoor konden hun individuele handelingen niet goed worden gevolgd en geregistreerd**.''

https://www.rdi.nl/actueel/nieuws/2022/08/30/tekortkomingen-in-beveiliging-van-aftapvoorziening-kpn - lees vooral het hele rapport. KPN is niet het slechtste bedrijf op dit vlak, vermoedelijk zelfs een van de betere. Maar de toegang tot de tapkamer was buitengewoon droevig georganiseerd. Dit is vrij typerend voor hoe dit soort dingen gaan.

Aftapvoorziening Vodafone niet voldoende beveiligd: boete van € 2,25 miljoen voor Vodafone

Nieuwsbericht | 22-10-2024 | 08:30

De Rijksinspectie Digitale Infrastructuur (RDI) heeft onderzoek gedaan naar de veiligheid van het aftapsysteem van Vodafone. Hieruit blijkt dat de beveiliging op meerdere onderdelen niet aan de wettelijke eisen voldeed. De RDI legt Vodafone daarom een boete op van in totaal € 2,25 miljoen.

https://www.rdi.nl/actueel/nieuws/2024/10/22/aftapvoorziening-vodafone-niet-voldoende-beveiligd

Do you think our lawful intercept systems are safe?

Ze zeggen het beleefd, maar hier staat “je firewalls en VPN machines worden steeds gehacked”

NOS

Overheden worden permanent gehackt en dat weten ze, maar daar zeggen ze meestal niet zoveel over.

— Bert Hubert, ex-toezichthouder inlichtingendiensten

Al vaak lek

Hubert noemt het "wel gek" dat Defensie nog steeds gebruikmaakt van het product van het bedrijf Fortinet, waarover het gaat in het rapport. "Dat is een bedrijf dat al zo vaak lek is gebleken: in 2023 180 keer. Dat is heel raar, want die producten zijn juist bedoeld om je te beschermen tegen aanvallen."

Hij vindt het dus vreemd dat de overheid nog vertrouwen heeft in Fortinet. "Het is alsof je een slot op je fiets plaatst dat er juist voor zorgt dat 'ie gestolen zal worden."

Heel vreemd is hoe organisaties stug spullen blijven kopen die bekend lek zijn. Zie ook de slide over “de kloof” - er worden hier beslissingen genomen door mensen die niet ‘s nachts uit bed gebeld worden als ze gehacked zijn.

Mitigerende maatregelen bij het gebruik van edge devices

Het NCSC en de Nederlandse inlichtingendiensten zien al langer een trend dat kwetsbaarheden in publiek benaderbare edge devices zoals firewalls, VPN-servers, routers en e-mailserververs worden misbruikt. Vanwege de uitdagingen op het gebied van beveiliging van edge devices zijn deze apparaten een geliefd doelwit voor kwaadwillenden. Edge devices bevinden zich aan de rand van het IT-netwerk en hebben geregeld een directe verbinding met het internet. Daarnaast worden deze apparaten vaak niet ondersteund door Endpoint Detection and Response (EDR) oplossingen.

Initiële compromittering van een IT-netwerk is moeilijk te voorkomen als de kwaadwillende hierbij gebruik maakt van een zero-day. Daarom is het van belang dat organisaties het 'assume breach'-principe hanteren. Dit principe hanteert dat een succesvolle digitale aanval al heeft plaatsgevonden of binnenkort gaat plaatsvinden. Op basis hiervan worden maatregelen genomen om de schade en impact te beperken. Denk hierbij aan het nemen van mitigerende maatregelen op het gebied van segmentering, detectie, incident response plannen en ↗ forensic readiness.

!!

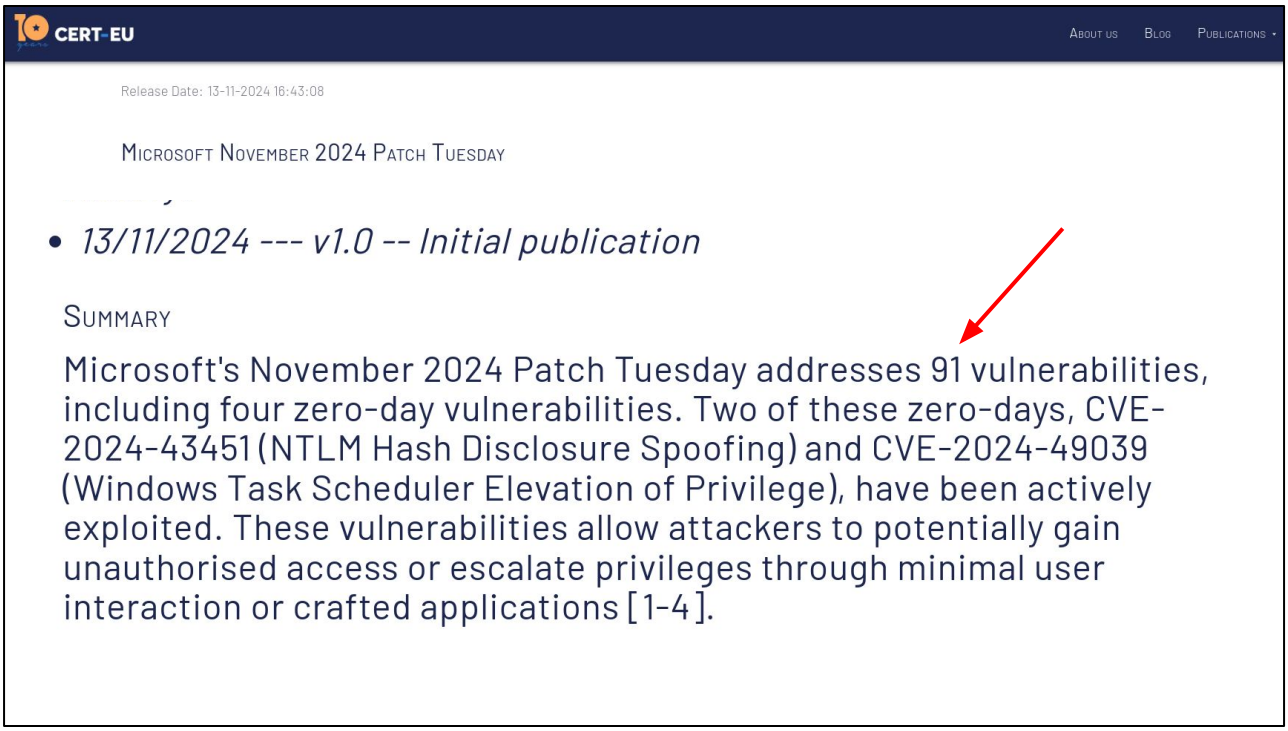
https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices - lees deze pagina goed, want er staat een diepe waarheid: ga er vanuit dat je al gehacked bent. Want meestal is dat ook zo. Maar tegelijk, als je een directie van een grote club vraagt hoe het zit met de security, dan is 'ie heel zeker dat het allemaal snor zit. Wederom de kloof.

Summary

On January 14, Microsoft has released its January 2025 Patch Tuesday updates, addressing a total of 159 security vulnerabilities across various products [1,2]. The patches include fixes for critical and important-severity issues that could allow attackers to gain unauthorised access, execute arbitrary code, or elevate privileges. Three vulnerabilities were already being exploited in attacks.

Technical Details

The eight (8) zero-day vulnerabilities resolved in this update are:



91 gaten in de “microsoft patch Tuesday”. Een “Zero day” is een beveiligingslek wat bekend is en waar ook al technieken beschikbaar zijn om er gebruik van te maken, terwijl er nog geen oplossing is.

Release Date: 09-10-2024 16:06:57

A A A A

Multiple Critical Vulnerabilities in Microsoft Products

Download

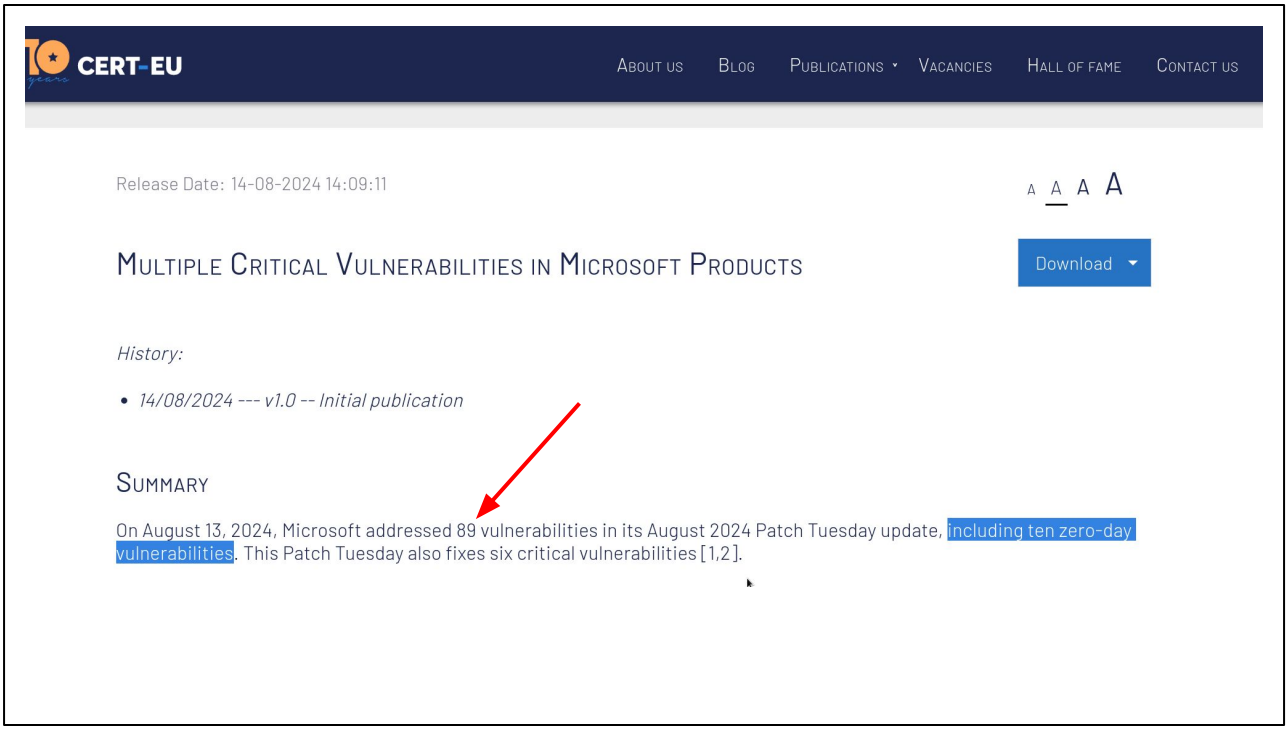
History:

- *09/10/2024 --- v1.0 -- Initial publication*

118!

Summary

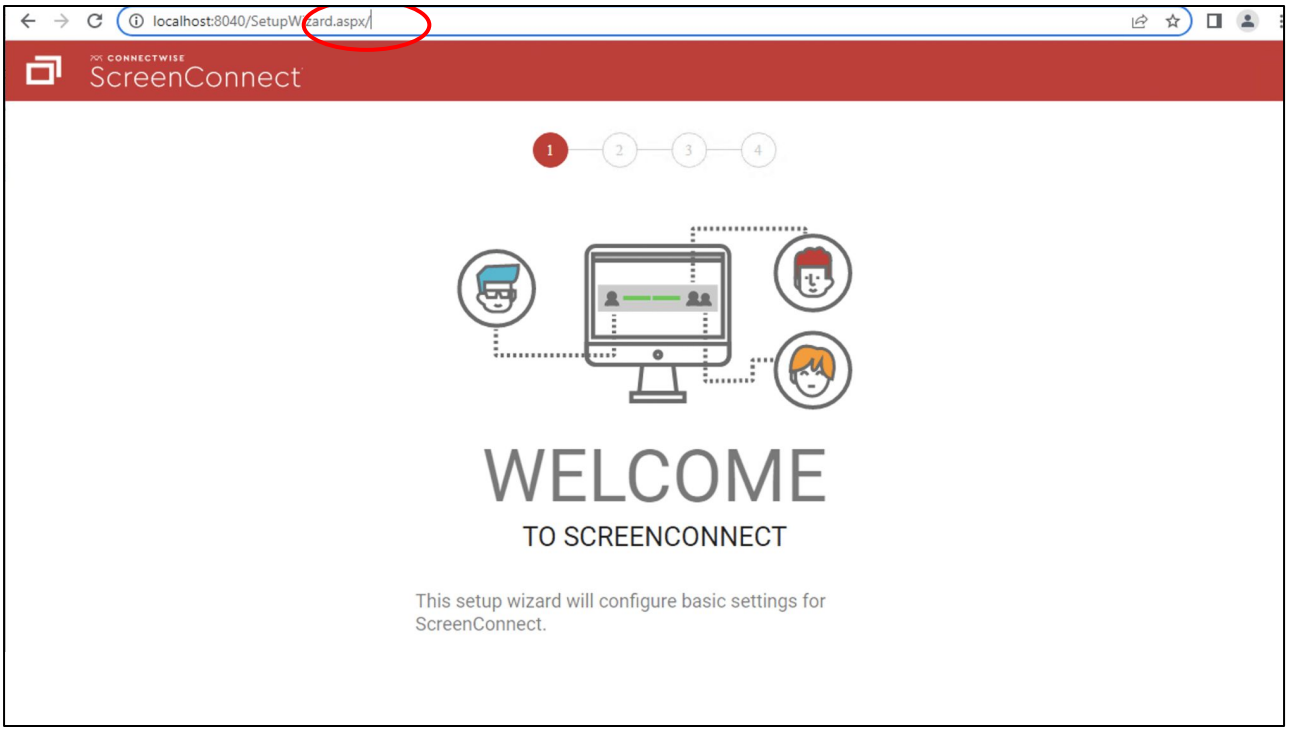
On October 8, 2024, Microsoft addressed 118 vulnerabilities in its October 2024 Patch Tuesday update, including five zero-day vulnerabilities. This Patch Tuesday also fixes three critical vulnerabilities [1,2].


CERT-EU
About us
Blog
Publications
Vacancies
Hall of fame
Contact us
Release Date: 14-08-2024 14:09:11
A A A A
Multiple Critical Vulnerabilities in Microsoft Products
Download
History:
14/08/2024 --- v1.0 -- Initial publication
Summary
On August 13, 2024, Microsoft addressed 89 vulnerabilities in its August 2024 Patch Tuesday update, including ten zero-day vulnerabilities. This Patch Tuesday also fixes six critical vulnerabilities [1,2].

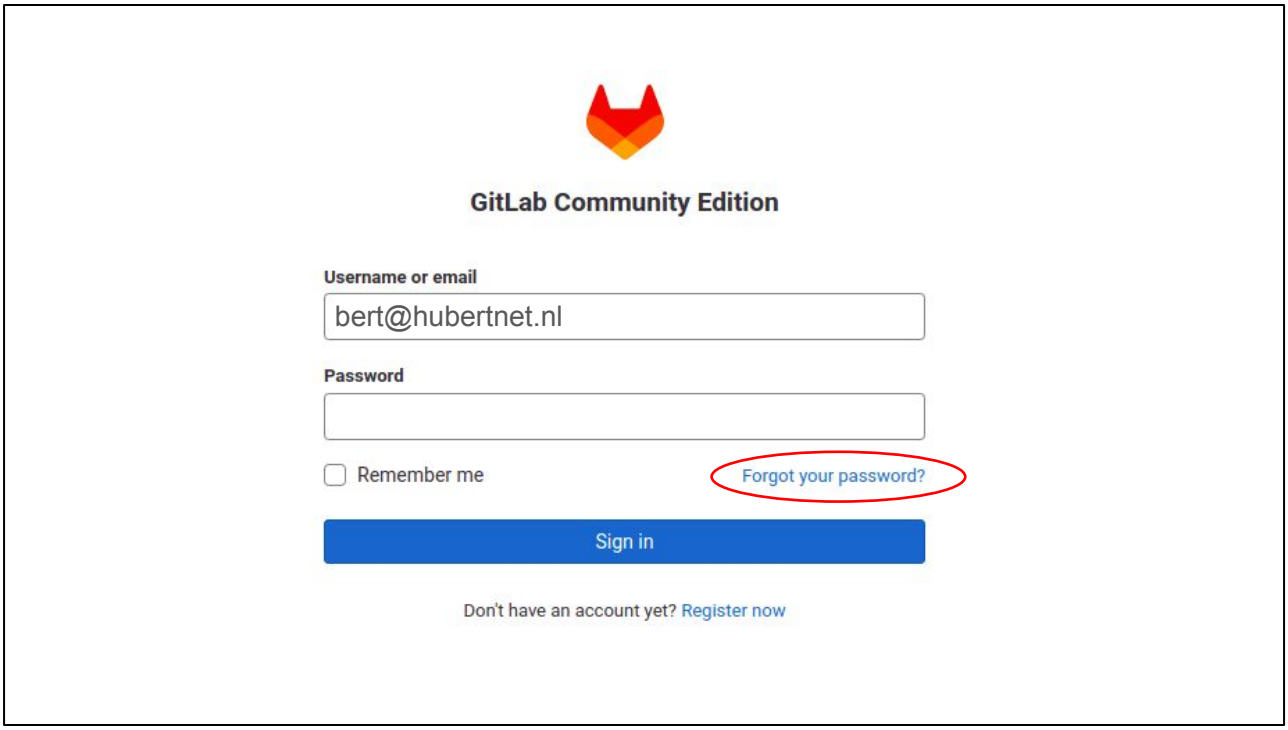
We see >100 major fixes/week

These issues had been there for years

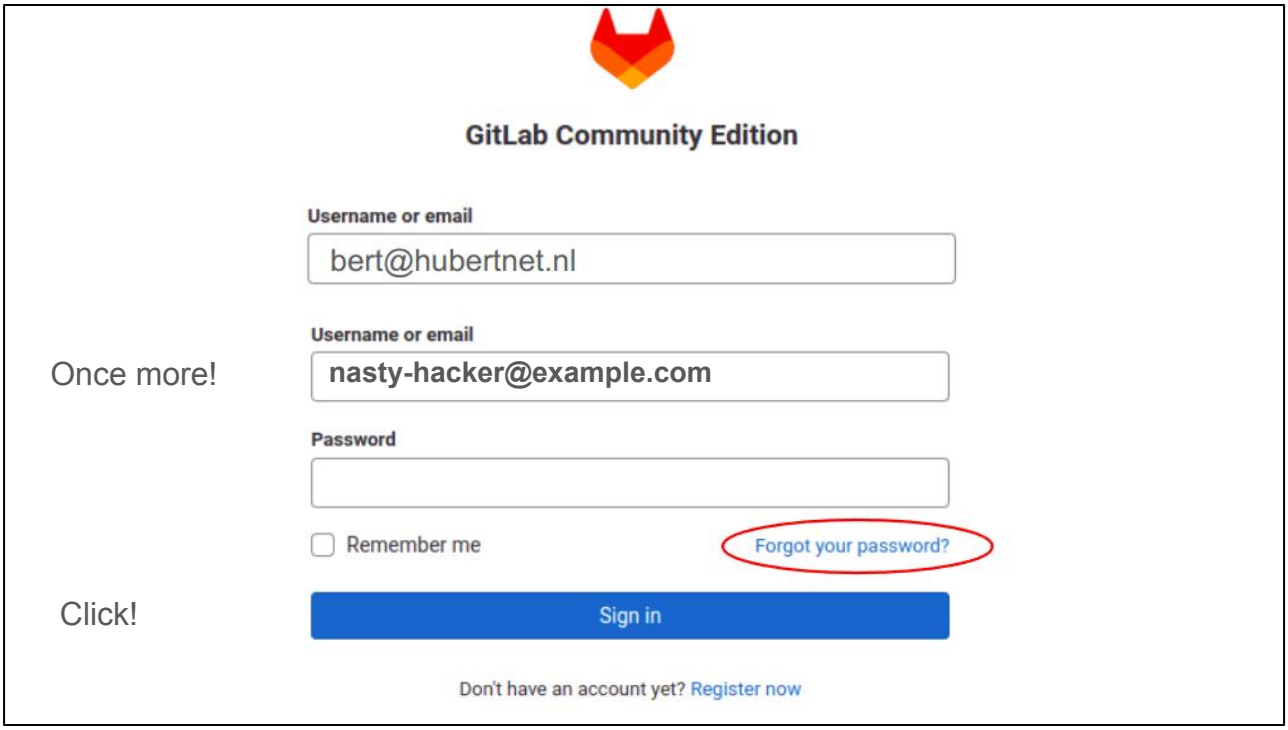
Not anywhere near done, we get 100 new problems/week!



Helpdesksoftware, te hacken door een enkele “/” toe te voegen aan het einde van de URL-bar. En dit is geen uitzondering, veel hacks zijn helemaal niet ingewikkeld. We hebben het nog niet voor elkaar.



GitLab is waar belangrijke bedrijven en overheden broncode en data opslaan. Hier, de ‘forgot your password’ knop



Als een aanvaller een extra regeltje aan dit formulier met een tweede email adres toevoegt, dan blijkt GitLab het *eerste* email adres te checken of je wel de systeembeheerder bent, EN DAARNA EEN RESET PASSWORD LINK TE STUREN NAAR HET TWEEDE EMAIL ADRES. Van de aanvaller dus.

Email scanner die checkt of je Excel sheet wel veilig is.. DOOR HEM UIT TE VOEREN.

NOS Nieuws Sport Live Programma's

Donderdag, 07:00

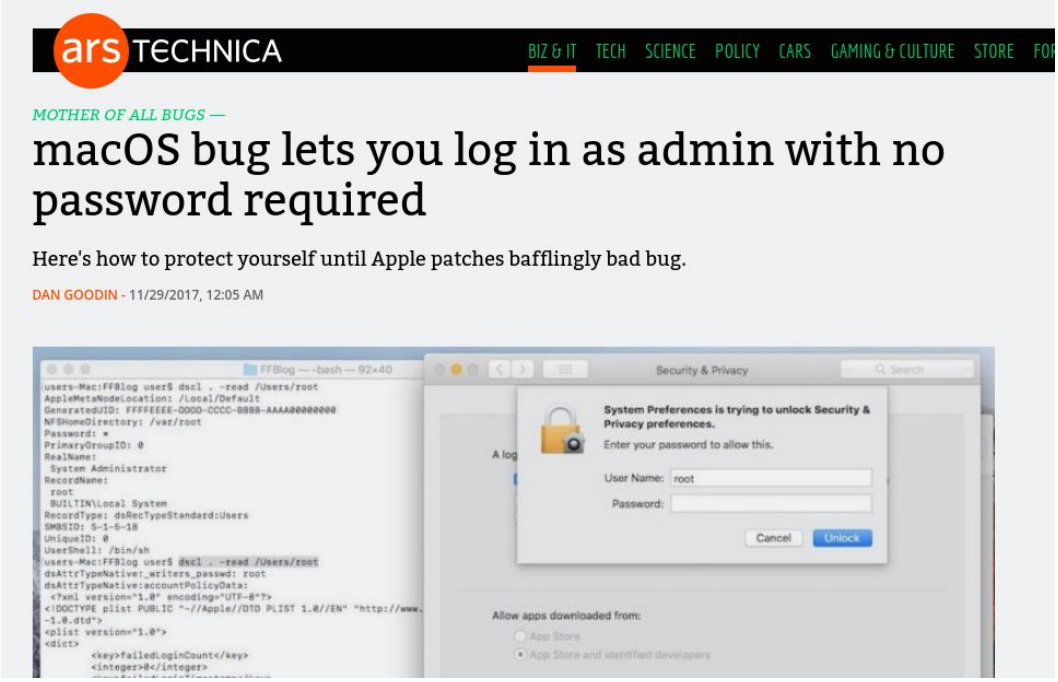
Ambtenaren gebruiken onveilig vergaderprogramma: 'Data waardevol voor spionnen'

274 **12 345 678**

De Nederlandse overheid is grootgebruiker van het videobelprogramma Webex. Uit Duits onderzoek blijkt dat dat programma niet zo veilig is als het belooft. Een journalist van de krant Die Zeit kon maandenlang gegevens verzamelen van tienduizenden videovergaderingen van overheidsfunctionarissen in heel Europa, ook van Nederlandse ministers. Tegen *Nieuwsuur* vertelt ze wat ze heeft ontdekt en waarom die data waardevol is voor spionnen of criminelen.

Voor vergaderingen op afstand gebruiken veel Nederlandse overheidsorganisaties het programma Webex, van de Amerikaanse techgigant Cisco. Het programma zou veiliger zijn dan andere populaire videobel-programma's als Zoom en Microsoft Teams. Toch lukte het Eva Wolfanger, techjournalist bij Die Zeit, maandenlang om informatie over tienduizenden Nederlandse vergaderingen te verzamelen. Waaronder ook vergaderingen van bewindslieden als demissionair ministers Hugo de Jonge en Dilan Yesilgöz.

Overheden vertrouwden op WebEx, die bleek z’n security af te laten hangen van een 7-cijferige code. Als je duizenden meetings houdt is het niet lastig om een 7-cijferige code te gokken/scannen.



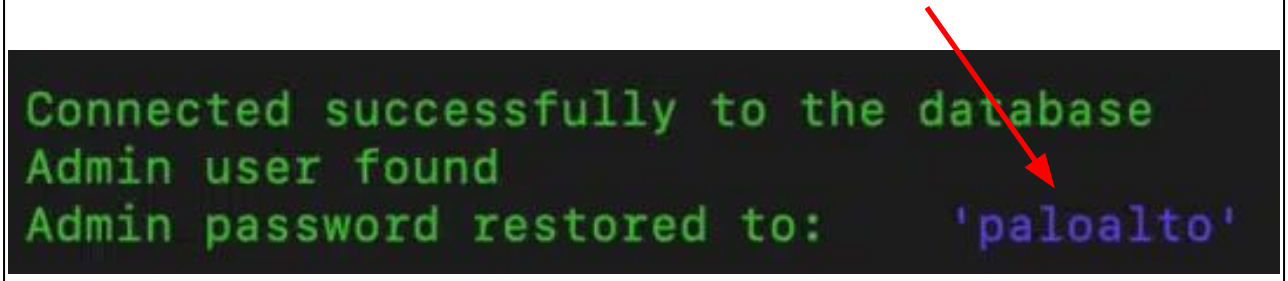
De bug van de eeuw. De headline vertelt het verhaal.

Palo Alto Networks: Leader in Cybersecurity Protection

by Zach Hanley | **Oct 9, 2024** | Attack Blogs, Attack Research, Disclosures

```
root@kali:~# curl -k 'https://10.0.40.64/OS/startup/restore/restoreAdmin.php'

✓       Connected successfully to the database
✓       Admin user found
✓       Admin password restored to:     'paloalto'
```



https://www.horizon3.ai/attack-research/palo-alto-expedition-from-n-day-to-full-compromise/

We counter this with the anti-phishing training

Het is dus allemaal vreselijk. En wie hebben we daarvoor de schuld gegeven? GEBRUIKERS! Want die klikken weleens op de verkeerde link. Maar we hebben daarmee geaccepteerd dat software ZO LEK is dat als je op 1 verkeerd knopje drukt iedereen gehacked is. Dit accepteren we niet van auto's of andere dingen. Als je auto ontploft als je de radio bedient in de derde versnelling worden we niet boos op de bestuurder maar op de fabrikant van de auto. Met software hebben we het decennia omgedraaid en dat kan echt niet meer. De anti-phishing training is een symptoom dat de arme gebruiker het maar op moet lossen.

"Unfortunately we have fallen prey to the myth of techno exceptionalism. **We don't have a cyber security problem – we have a software quality problem**. We don't need more security products – **we need more secure products**."

Jen Easterly, former Director of the US Cybersecurity and Infrastructure Security Agency

Let’s head to the cloud then?

Microsoft faulted for ‘cascade’ of failures in Chinese hack

The independent Cyber Safety Review Board’s report knocks the tech giant for shoddy cybersecurity practices, lax corporate culture and a deliberate lack of transparency

By Ellen Nakashima and Joseph Menn

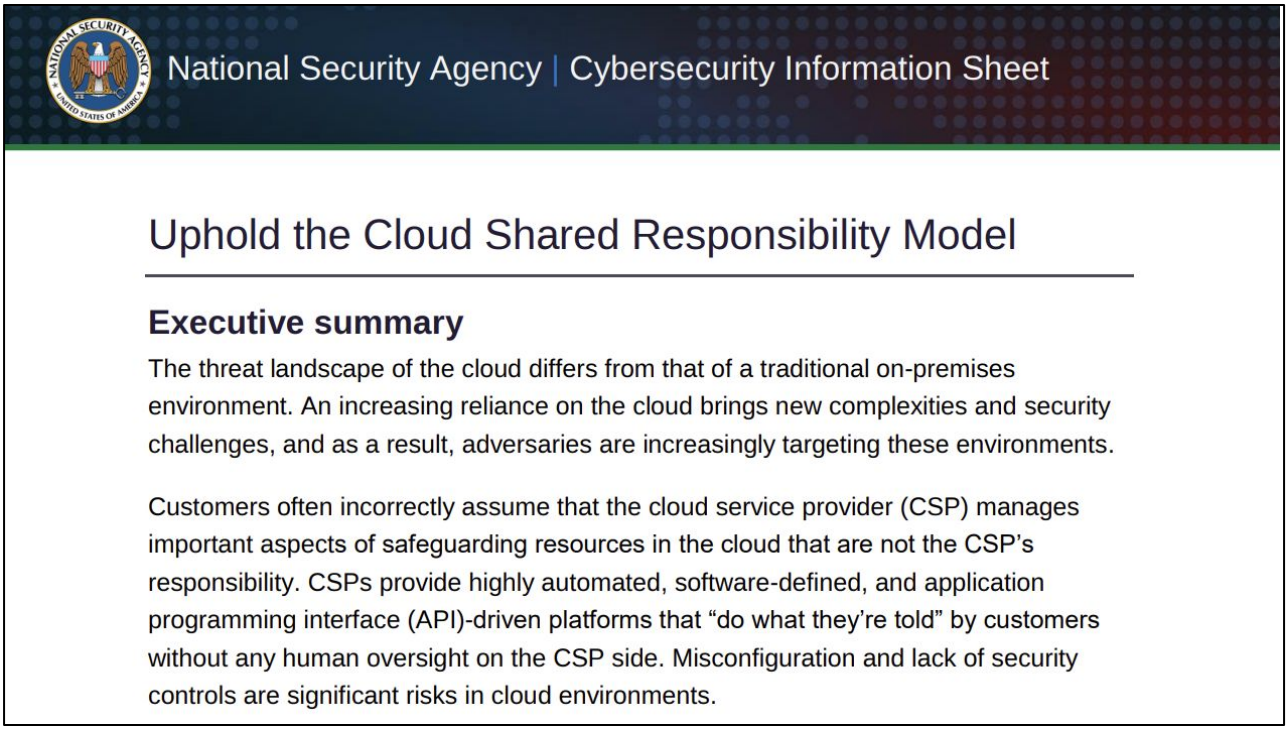
Updated April 2, 2024 at 6:18 p.m. EDT | Published April 2, 2024 at 4:00 p.m. EDT

https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/ - de Microsoft cloud zit vol met Chinese hackers, en ze krijgen die er niet uit. Het viel niet mee.

After years of touting the strength of its cybersecurity, Microsoft — the world's most valuable company — has been beset by recent embarrassing breaches. In early 2021, Chinese government-sponsored hackers compromised Microsoft Exchange email servers, putting at risk at least 30,000 public and private entities in the United States along with at least 200,000 worldwide.

In January, Microsoft detected an attack on its corporate email systems by the Russian foreign spy service, the SVR. The company said the spies broke into a testing unit, moving somehow from there into emails of senior executives and security personnel. Microsoft alerted its customer Hewlett-Packard Enterprise that it had been hacked as part of that campaign, and U.S. officials told The Post last month that there were dozens of other victims, including Microsoft resellers.

https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/ - Russen en Chinezen in je cloud.



https://media.defense.gov/2024/Mar/07/2003407863/-1/-1/0/CSI-CloudTop10-Shared-Responsibility-Model.PDF - zeer de moeite waard. Als je je software in de cloud draait kan die nog steeds gehacked worden. Maar de aanname is juist vaak dat “het in de cloud veilig is”. Maar dat is de belofte niet. Je huurt een computer, geen beveiligingsbedrijf.

Computer security is pants. And if you outsource your systems, your security will be pants **somewhere else.** Except now easier to ignore.

Confidentiality
Integrity
Availability

Not just about our privacy.

https://berthub.eu/articles/posts/niks-te-verbergen-wel-steeds-meer-uit-te-leggen/

A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

https://www.wired.com/story/oldsmar-florida-water-utility-hack/ - dit was dus Echt Eng

https://www.cisa.gov/water

Free Cyber Vulnerability Scanning for Water Utilities

CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.

EPA Water Resilience Cybersecurity Help Desk

EPA's help desk is available 24/7 and responds to water cyber inquiries within two days. The help desk provides guidance to help prevent, detect, respond to and recover from cyber incidents.

EPA Free Cybersecurity Assessment Service

EPA conducts free cyber assessment for drinking water and wastewater utilities using EPA's Cybersecurity Checklist derived from CISA's CPGs. Utilities receive a summary report and a Risk Management Plan to help in prioritizing cybersecurity efforts.

Of je sluit je waterleiding niet aan op het internet? Kennelijk moet het gewoon… Dus dan maar adviezen hoe het veilig kan.

https://berthub.eu/articles/posts/cybersecurity-is-like-food-safety/

How did we get here?

- **Amateur hour**
- For dangerous chemicals, industrial plants, power plants, we've developed rules and legislation
  - Over the centuries
  - Pre-Titanic, everyone could just design a ship
- **We've moved to computers faster than we could craft rules**
  - And we're still not ready
- Security is not something that gets you a promotion
  - Best you can achieve is "not fail dramatically"
- Boards of directors in The Netherlands and Europe are mostly devoid of technical knowledge
- Boards therefore prefer to outsource

- **NEW: Legislation like NIS2 directive (NCSC), CRA (RDI), DORA, PLD…**

Cyberbeveiligingswet

Economie *Openbare orde en veiligheid* *Ruimte en infrastructuur*

In het kort

Dit wetsvoorstel implementeert de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Dit doel wordt in Nederland bereikt door, ter implementatie van deze richtlijn, in dit wetsvoorstel onder meer verplichtingen op te leggen aan die entiteiten, zoals het treffen van adequate beveiligingsmaatregelen en het melden van ICT-incidenten.

Naast deze internetconsultatie vindt ook de internetconsultatie plaats van de Wet weerbaarheid kritieke entiteiten. Ga hiervoor naar https://www.internetconsultatie.nl/wetweerbaarheidkritiekeentiteiten/b1

Reageren op deze consultatie →

NIS2/ Cyberbeveiligingswet biedt een beetje hoop

Tussen april en september 2025

Vervolgens laten Jetten en Yesilgöz-Zegerius weten: "Ter implementatie van NIS2-richtlijn zal naar verwachting in het tweede of derde kwartaal van 2025 de Cyberbeveiligingswet in werking treden." Daarmee wordt de door de EU gestelde deadline voor implementatie in nationale wetgeving flink overschreden. Begin dit jaar heeft de demissionaire minister van Justitie en Veiligheid al laten weten dat de deadline van 17 oktober dit jaar niet gehaald gaat worden.

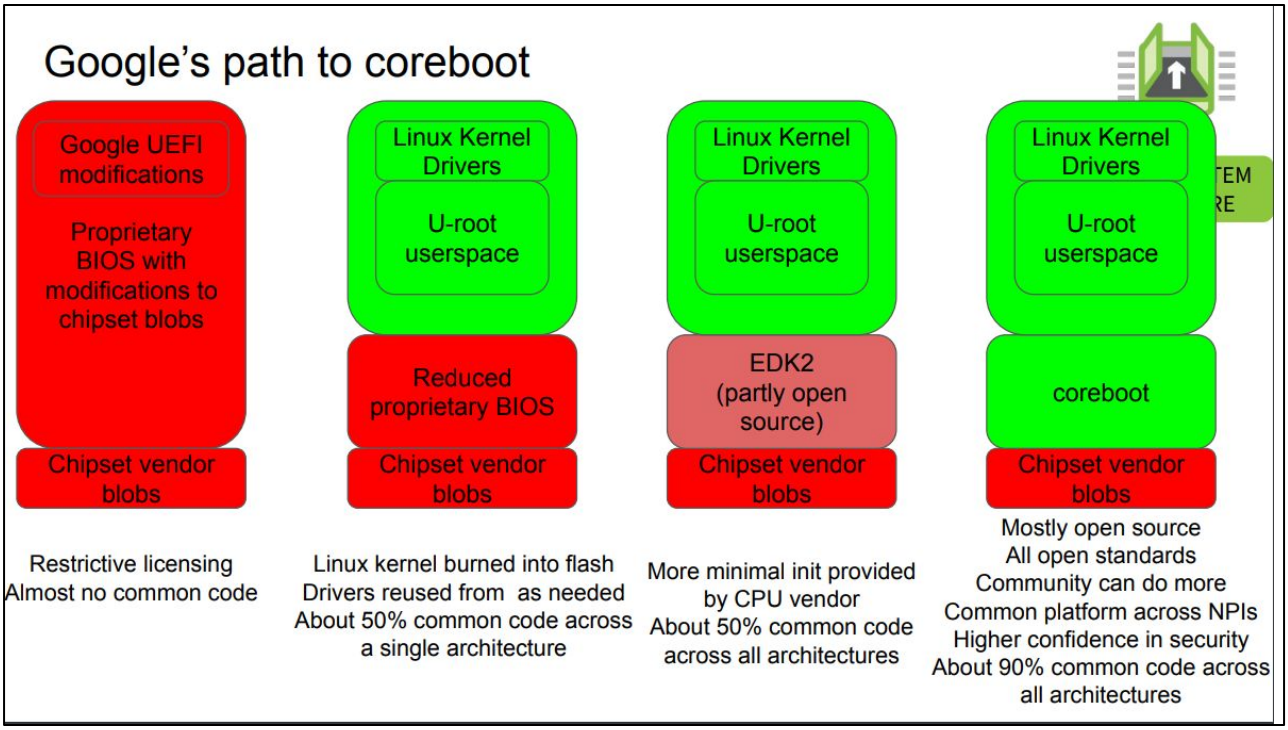
https://www.agconnect.nl/maatschappij/security/nis2-komt-pas-over-een-jaar-of-net-meer-in-nederlandse-wet - maar we geloven er nog steeds niet echt in. Kan ook best in 2026.

Meanwhile…

ANDY GREENBERG SECURITY MAY 31, 2023 9:00 AM

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Hidden code in hundreds of models of Gigabyte motherboards invisibly and insecurely downloads programs—a feature ripe for abuse, researchers say.



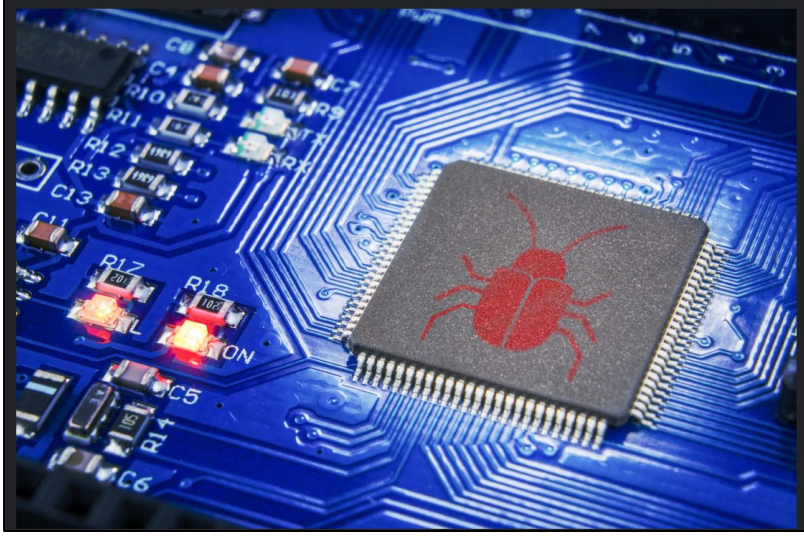
https://146a55aca6f00848c565-a7635525d40ac1c70300198708936b4e.ssl.cf1.rackcdn.com/images/9ef86592bcfed261f7018977d5cbe752a529216d.pdf

FACEPALM GOES HERE

Secure Boot is completely broken on 200+ models from 5 big device makers

Keys were labeled "DO NOT TRUST." Nearly 500 device models use them anyway.

DAN GOODIN – JUL 25, 2024 8:00 PM 201



The researchers soon discovered that the compromise of the key was just the beginning of a much bigger supply-chain breakdown that raises serious doubts about the integrity of Secure Boot **on more than 300 additional device models from virtually all major device manufacturers**

https://arstechnica.com/security/2024/07/secure-boot-is-completely-compromised-on-200-models-from-5-big-device-makers/

SYNful Knock - A Cisco router implant - Part I

September 15, 2015

Mandiant

“The initial infection vector does not appear to leverage a zero-day vulnerability”

Written by: Bill Hau, Tony Lee, Josh Homan

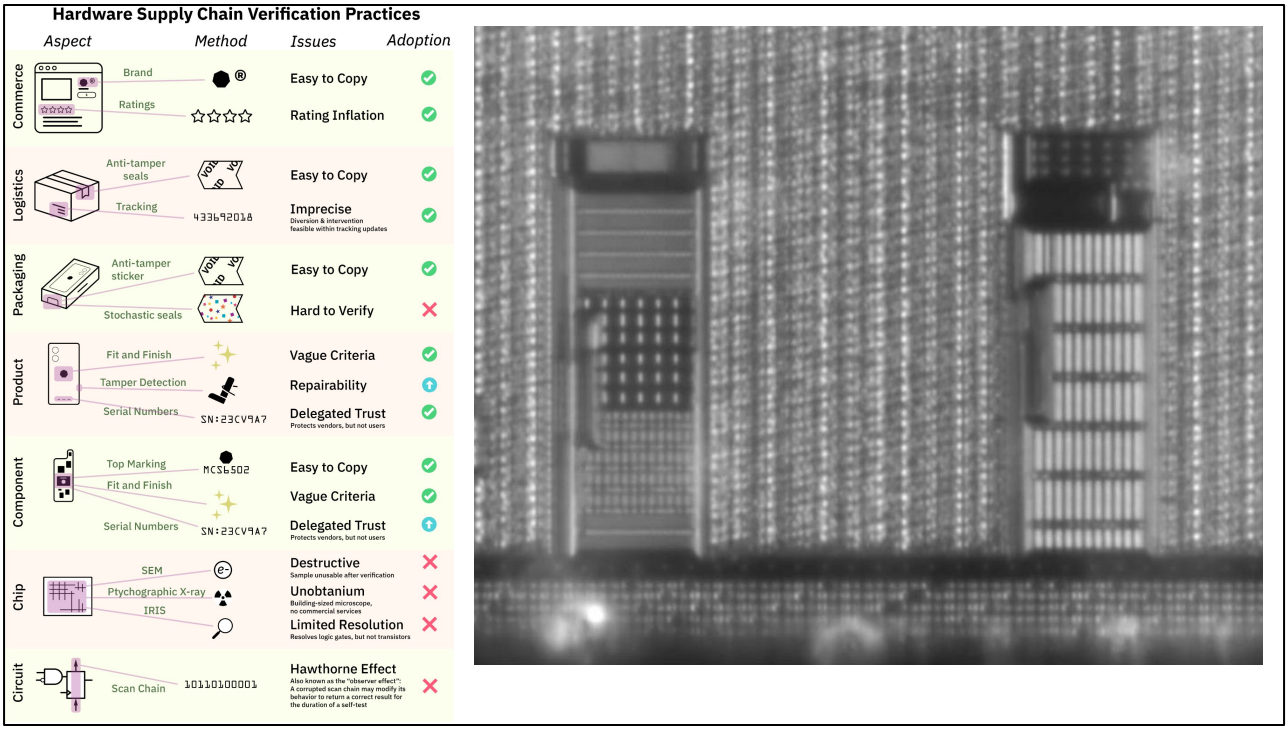
Overview

Router implants, from any vendor in the enterprise space, have been largely believed to be theoretical in nature and especially in use. However, recent vendor advisories indicate that these have been seen in the wild. Mandiant can confirm the existence of at least 14 such router implants spread across four different countries: Ukraine, Philippines, Mexico, and India.

SYNful Knock is a stealthy modification of the router's firmware image that can be used to maintain persistence within a victim's network. It is customizable and modular in nature and thus can be updated once implanted. Even the presence of the backdoor can be difficult to detect as it uses non-standard packets as a form of pseudo-authentication.

The initial infection vector does not appear to leverage a zero-day vulnerability. It is believed that the credentials are either default or discovered by the attacker in order to install the backdoor. However, the router's position in the network makes it an ideal target for re-entry or further infection.

https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis/



https://www.bunniestudios.com/blog/2024/iris-infra-red-in-situ-project-updates/

Finally, a big shout-out to NLnet and the European Commission. NLnet's NGI0 Entrust fund, established with support from the European Commission's Next Generation Internet Program, are instrumental in facilitating my work on IRIS. Also a big shout-out to my Github Sponsors for their incredible generosity and monthly support. Thanks to all these donors, I'm able to keep IRIS 100% open source and free of conflicts of interest with commercial investors.

❤️ Sponsor me on Github! ❤️

Are you doing in situ inspection of your chips?

Do you run custom BIOS to evade hundreds of binary blobs of unknown provenance?

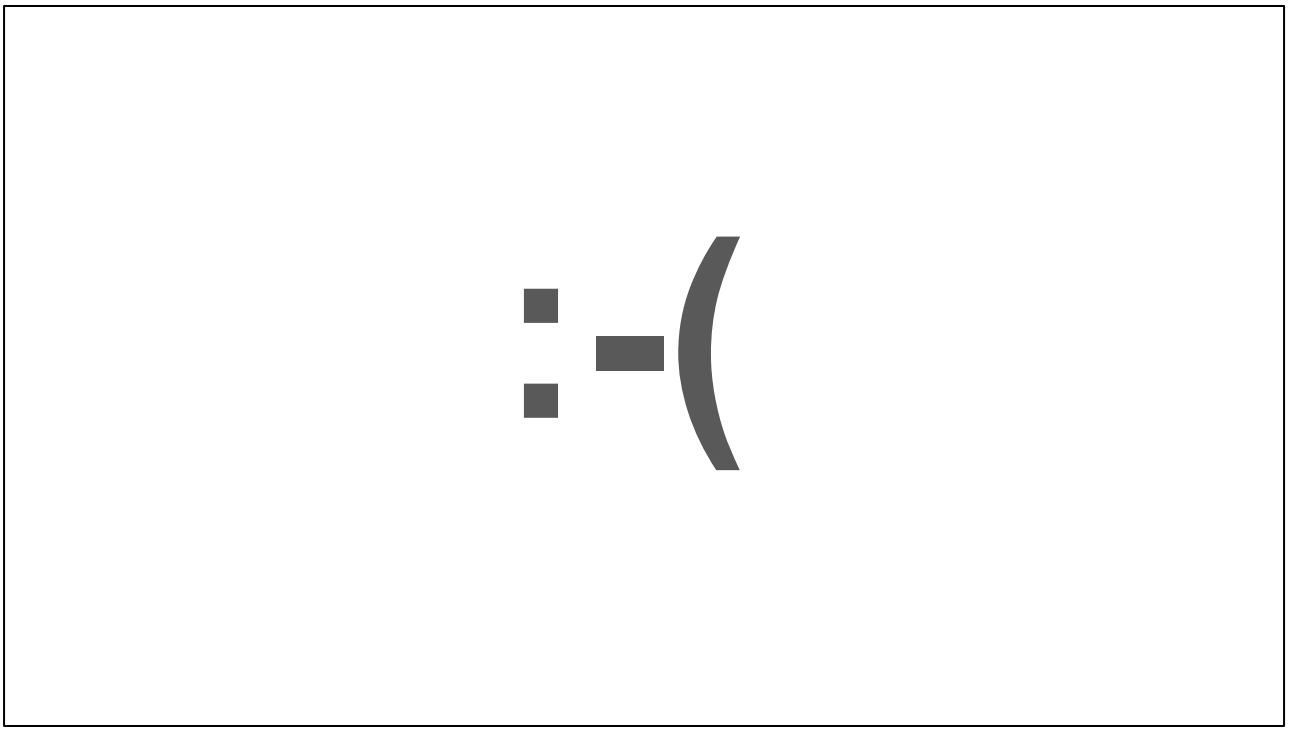
Did you upgrade the firmware to restore the (weak) protections of secure boot?

Did you inspect the memory of your routers & switches recently?

Did your vendor do all this?

No, we're not even close to doing that.

Still, tomorrow we'll go back to thinking our networks are secure!



However..

- Banks, financial institutions, governments still have an impressive track record of not getting hacked
- And the reasons are obvious:
  - Keep track of what services you run
  - Procedures to decide what they DO run
  - Updates, updates, updates!
  - Monitoring

- So please don’t give up because the state entities might be sending you hardware with implants
  - You still need to keep out the less skilled attackers

- But also lie awake at night if you don’t know where that firmware came from, or if no one in your org knows what a binary blob is!

The terrible state of cyber security

A reality check

Bert Hubert
bert@hubertnet.nl

https://berthub.eu/amsec7