I. Close the (exploit) window! Why users should update Chrome for Windows immediately

On 25 October 2022, Google launched version 107 of the most widely used web browser, which has a market share of over 41%. Users of Windows versions older than 103.0.5060.114 are strongly advised to install the update. According to browser statistics provided on stetic.com, together these versions rank seventh among the most-used browsers. However, these versions also contain four security vulnerabilities, three of which Google rates as ‘high-risk’. Back in July, security researchers from Avast discovered and reported a high-risk security vulnerability (CVE-2022-2294) in a collection of web communication protocols for which malware is already in circulation. By issuing the security update mentioned above, Google is closing three additional security vulnerabilities, two of which are also classified as ‘high-risk’: CVE-2022-2295 affects the V8 JavaScript engine, allows access from outside the memory allocation and can lead to implanted malware being executed. CVE-2022-2296, another high-risk vulnerability, was discovered in a Chrome OS shell. The update also closes another, unspecified security vulnerability.
Since people generally use browsers several times a day, it is important they ensure that they always keep them up to date – whichever one they use. If you’d like to check which version of Chrome you’re currently using to surf the net, you can do so in the ‘About Google Chrome’ window. To navigate there, click on the kebab menu (the three vertical dots), which can be found next to the address bar on the far right of the browser window, followed by ‘Help’ at the bottom of the menu window that appears, and then finally ‘About Google Chrome’.

Google documents the browser’s current state of development on ‘chrome-releases.googleblog.com’ at the address linked below.

Read more:
https://www.itmagazine.ch/artikel/77491/Dringendes_Update_Kritisches_Chrome-Leck_wird_bereits_ausgenutzt.html
https://www.stetic.com/de/market-share/browser/
https://chromereleases.googleblog.com/2022/10/beta-channel-update-for-chromeos_20.html

II. A never-ending story? Microsoft fails to close security gaps in the Exchange Server

Microsoft is currently reporting a large number of attacks on several of its programs and systems and has released security updates for Azure, Office, Windows and SharePoint. Despite taking such action, the Richmond-based software giant apparently appears unable to close two vulnerabilities in the Exchange Server – CVE-2022-41040 (rated ‘high-risk’) and CVE-2022-41082 (classified as ‘medium-risk’). Although both vulnerabilities have been targets of attacks since the end of September, Microsoft has not released any patches to date. The customer guidance that Microsoft publishes in the blog run by its very own Security Response Center (see the first link below) documents a rather unhelpful range of ever-new workarounds instead of a functional security update. It is currently unknown when this update will be released. The two vulnerabilities allow attackers to introduce and execute malware. Although they have to authenticate themselves to perform such actions, this has so far not proved impossible for professional attackers and remains the case.

Because of this issue, the Azure security leak CVE-2022-37968 is also assigned the highest risk level (a CVSS score of 10 out of 10). Even though attackers need to know the randomly generated DNS endpoint to penetrate Azure Arc-enabled Kubernetes clusters, once they do so they can then take over the entire cluster with all the administrator privileges.

Attackers are also granted system privileges if they gain access through vulnerability CVE-2022-41033 in Windows’ COM+ Event System. Cybercriminals could use the other critical
vulnerabilities to introduce and execute malware on SharePoint servers or to gain higher user permissions in Active Directory.

Users should therefore definitely install the security updates provided. In the case of the Microsoft Exchange Server, unfortunately, all we can do at present is cling to hope.

At the end of September, the corporation experienced first hand what can happen if a Microsoft endpoint isn’t adequately protected: SOCRadar, a security firm, informed Microsoft that 2.4 TB of data belonging to 65,000 companies in 111 countries had been made public – including more than 335,000 emails, data from 133,000 projects and 548,000 user records. While Microsoft did indeed confirm the leak in principle in its own statements, it also put the extent of the damage and the number of people affected into perspective. Microsoft has since closed the vulnerability itself.

Read more:
https://t3n.de/news/microsoft-datenleck-2-4-tb-daten-oeffentlich-1507314/
https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location/2/

III. Everything’s bigger in China: 2 billion data records allegedly stolen from TikTok

So much for the ‘Middle Kingdom’! In China, many things take on the superlative form. And compared to the 548,000 user records affected by the Microsoft data theft described above, the 2,000,000,000 (two billion!) data records that hackers allegedly got their hands on (in addition to the app’s source code) during an attack on the US branch of TikTok, the Chinese social media app, are on a whole different level entirely. bleepingcomputer.com reported on this incident in early September.

To this day, TikTok denies reports that it suffered a data leak or fell victim to a hacker attack, choosing to stress instead that the data is publicly accessible. BeeHive, an independent cybersecurity platform, has on the other hand analysed data leaked to it and confirmed the hack.

So, even though there seem to be more arguments than admissions doing the rounds at the moment, there’s no harm in TikTok users checking their accounts, changing their passwords and activating two-factor authentication.

Read more:
IV. Hacking – a ‘sweet’ job: Läderach, a Swiss chocolatier, fell victim to a ransomware attack launched by a new, aggressive group of hackers operating under the name BianLian

For the Swiss, it was almost an attack on critical—or, at least, systemically relevant—infrastructure. On 6 September, inside-it.ch reported a ransomware attack on Läderach, a Glarus-based chocolatier. Production, logistics and administration were particularly affected by the attack. The company immediately brought in the National Cybersecurity Centre (NCSC), not to mention relevant investigative and law enforcement agencies, after becoming aware of the incident.

At that point, it was also still completely unclear whether the attack was limited to a pure blackmail attempt or whether data had been stolen too. In mid-September, Läderach acknowledged that the BianLian hacker group might have successfully accessed employee data, which is why the data subjects who might have been affected were informed.

It has since become clear that BianLian didn’t stop at the blackmail attempt. It also stole management documents, data relating to products and future projects, budget plans and personal data from the company’s HR department and published them on the dark web.

Since September 2022, organisations have been issuing warnings galore about the rapidly expanding cybergang, which [redacted], a US cybersecurity firm, described as a ‘group of individuals who are very skilled in network penetration but are relatively new to the extortion/ransomware business’. For their new field of business, the criminals use a toolbox they developed themselves—namely encryption programs and backdoors. These programs and backdoors, not to mention the command-and-control software, are written in Go.

[redacted] went on to warn that we can expect to see an explosive spread in the group’s crimes.

The blackmailers aren’t just after money. They are also keen to get their hands on ‘financial, client, business, post, technical and personal files’, since they themselves write in the instruction file that appears as ‘Look at this instruction.txt’ on the monitors of hacked systems. This ransom note is shown in Blackberry’s cybersecurity blog post, which discusses the new threat at length, going into technical detail and also explaining that the hackers adopted the name BianLian from the ancient dramatic art associated with Chinese theatre, specifically opera originating from the Szechuan Province. ‘BianLian’ means ‘face changing’ and is
considered the highlight of Szechuan opera. Actors and actresses wear elaborate, brightly coloured masks, which they change in the blink of an eye to take on a new role. The mechanisms behind this art form were long considered a closely guarded secret, and revealing the secret was just as punishable as the actions of the BianLian hacker group are today ...

Read more:
https://www.inside-it.ch/schoggifabrikant-laederach-von-ransomware-attaque-betroffen-20220906
https://www.swisscybersecurity.net/cybersecurity/2022-09-08/cyberkriminelle-attackieren-schweizer-schogg

V. Uber – it just happened again: 18-year-old completely compromises the ride-on-demand service

When Britney Spears released her second studio album, ‘Oops!... I Did It Again’ in the year 2000, she was just 19 years old – and the foundation of Uber was still nine years away. Now, an 18-year-old has hacked the billion-dollar ride-hailing service and compromised almost every aspect of it. And this less than five years after it was revealed that data belonging to more than 50 million passengers had been stolen in 2016. Uber faced a barrage of criticism over its attempts to cover up the breach at that time. Uber’s then security chief was dismissed and had to stand trial for covering up a crime.

To quote Britney Spears, ‘Oops!... I Did It Again’. In mid-September, Uber reported that it had once more been hacked. According to his own statements, the unknown hacker tricked an employee into giving out their login credentials through social engineering and thereby gained almost unlimited access to all of the ride-hailing service provider’s cloud-based systems. Among other information, Uber stored sensitive customer and financial data in the cloud – and to prove that fact, the young hacker sent screenshots documenting the breach to several security researchers. One of the security researchers told the New York Times after reviewing the information sent to him that the hacker had ‘virtually unlimited access’ to all the systems. He believed that Uber was ‘completely compromised’.

The hacker described himself as an 18-year-old with a few years of hacking experience, before going on to explain he had attacked the company for doing too little for cybersecurity and not paying its drivers enough. In a statement made on 19 September, Uber linked the attack to the Lapsus$ hacking group, pointing out that the same hacker had also attacked the video game developer ‘Rockstar’ on 13 September 2022.

Four days later, London police announced in a short tweet that they had arrested a 17-year-
old on suspicion of hacking. Since it was extremely unusual for an announcement like this to be made concerning the arrest of a single hacker, Der Spiegel suspected that the arrested individual might be the perpetrator or one of the perpetrators responsible for the Uber and/or Rockstar hacks.

Read more:

https://www.netzwoche.ch/news/2022-09-16/cyberkriminelle-attackieren-uber
https://www.npr.org/2022/09/16/1123578408/uber-data-breach-hack
https://techcrunch.com/2022/09/16/uber-internal-network-hack
https://www.uber.com/newsroom/security-update
https://www.spiegel.de/netzwelt/netzpolitik/fall-lapsusse-londoner-polizei-nimmt-17-jahrigen-mutmasslichen-hacker-fest-a-67394b41-13e7-4a25-8d01-0d207a7687f

VI. Burn, baby, burn: firewood from fake shops

The story’s always the same: when rising demand drives prices up and availability down, crooked characters come out of the woodwork too. In the May/June 2022 issue of the Security Report, for instance, we warned that the lack of availability of bicycles would lead to new fake shops popping up online, offering bicycles that are either sold out or listed at prices well below average, but never delivering the bicycles that customers had ordered – and paid for.

Now, resourceful racketeers have apparently chosen wood as the product for their next money-making scam. Why? Because in the wake of the announced energy crisis, the prices of firewood and pellets have skyrocketed too. Many orders can no longer be processed because suppliers are simply out of stock. But anyone who thinks they’ve found a superb solution on a supposedly cheap firewood shop on the internet should make sure it’s not their own money that they’re burning. The consumer advice centre in the German state of Lower Saxony warns that pellets and firewood are a rehash of the scams we saw relating to gardening products, wicker beach chairs and bicycles during the coronavirus crisis. Shady suppliers or crafty criminals took advantage of the crisis to either offer goods in online shops at immensely overinflated prices or even to cash in on them in fake shops. The list of all the fake shops known to consumer protection agents in northern Germany has grown to a respectable length and can be found on the Lower Saxony consumer advice centre’s website (linked below).

In Switzerland, gangs of fraudsters from Benin are taking an even more subtle approach. They are using fake profiles and invoices to offer firewood at bargain-basement prices on Facebook Marketplace. While the Swiss Farmers’ Union currently recommends paying prices of between CHF 170 and CHF 210 for log burner-ready beech wood, the fake offers are significantly lower, at around CHF 100 per stere of beech wood. What makes this scam a particularly nasty one is the fact that the Beninese scammers use data belonging to previous victims. In its article
published on 8 September, *Der Beobachter* describes the case of a woman who had submitted her data while looking to take out a loan in 2020. At that time, the West African criminals used the victim’s data to launder money and commit other fraud for which she ended up being convicted in Switzerland. Now, history could repeat itself – only this time due to firewood fraud.

*Der Beobachter* therefore advises that people exercise extreme caution if offers seem too good to be true on Facebook Marketplace. And the Swiss National Cybersecurity Centre (NCSC) has also compiled a list of measures that people can take against dubious online shops and published it at the link below.

Read more:

https://www.verbraucherzentrale-niedersachsen.de/vorsicht-falle
https://www.sbv-usp.ch/de/preise/direktvermarktung/brennholz

This SWITCH Security Report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH Security Report does not represent the views of SWITCH; it is a summary of various reports published in the media. SWITCH assumes no liability for the content or opinions presented in the Security Report nor for the correctness thereof.