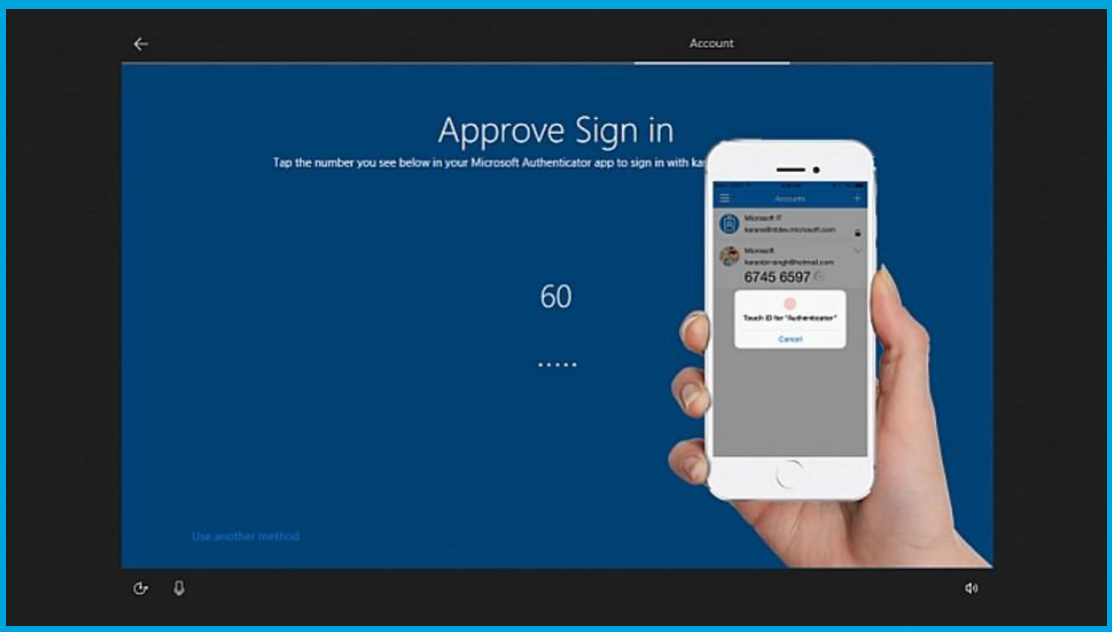
kindred

Security Newsletter

12 February 2018

Subscribe to this newsletter

Microsoft Tries to Ditch Passwords In New Version Of Windows 10



Passwords are a huge headache for most computer users. There are so many to keep tabs on that it wears people out mentally. Microsoft wants to ease that burden, even if it's only by a single password. The company has just released a new version of Windows 10 that ditches the log-in password in favor of less bothersome alternatives. You can sign in with your fingerprint, your face, or a PIN.

To be clear, those are all existing ways that you can sign in to Windows 10. The difference is that this version doesn't require you to setup a password first and then switch to one of the other options. That step has been removed. In the new version, you simply tap a notification on your phone to authorize your account.

Install Microsoft Authenticator on your phone and sign in with your Microsoft account. Sign in with the same account on your computer. When Microsoft sees that you're trying to sign in, it will send an alert to your phone and ask you to approve the request.

For now, Microsoft has limited the tap-to-sign-in functionality to Windows 10 S. That's a special mode that only allows users to install apps that are listed in the Windows Store. While it does have some clear security benefits, using "S Mode" does mean that you won't be able to install apps from third party sources. That includes apps like Chrome, Firefox, Steam, and iTunes.

Read More

WordPress Holds "Epic Fail Week" —Devs Break Background Updates, Ignore Zero-Day

WordPress version 4.9.3 was released earlier this week with patches for a total 34 vulnerabilities, but unfortunately, the new version broke the automatic update mechanism for millions of WordPress websites. WordPress team has now issued a new maintenance update, WordPress 4.9.4, to patch this severe bug, which WordPress admins have to install manually.

Thus, WordPress administrators are being urged to update to the latest WordPress release manually to make sure they'll be protected against future vulnerabilities. To manually update their WordPress installations, admin users can sign into their WordPress website and visit Dashboard→Updates and then click "Update Now."

Moreover, the company released two new maintenance updates this week, but none of them includes a security patch for a severe application-level DoS vulnerability disclosed last week that could allow anyone to take down most WordPress websites even with a single machine.

Read More

Even More

Hackers Pounce on Cisco ASA Flaw (CVE-2018-0101)

Five days after details about a vulnerability in Cisco ASA software became public, hackers have now started exploiting this bug in the wild against Cisco ASA devices. Cisco did not provide any details about the exploitation attempts or the techniques hackers used, but only said it was "aware of attempted malicious use of the vulnerability."

The exploited bug is CVE-2018-0101, a vulnerability that became public in late January. Initially, it was believed that only Cisco devices running ASA software with the VPN (webvpn) feature enabled were vulnerable, but more components were found to be vulnerable later.

Companies rushed to patch the issue, but by Monday this week, Cisco reissued security updates to deliver additional patches. According to a security advisory the company is maintaining, Cisco said engineers discovered that the bug was far more wide-reaching than initially thought. The update introduced additional exploitation vectors, and Cisco users are advised to update their ASA-based devices again, with Cisco's updated patch.

Read More

Uber data breach aided by lack of multi-factor authentication

Uber quits GitHub for in-house code after 2016 data breach. Code trove wasn't to blame: Uber didn't have multifactor authentication on repos that included AWS credentials.

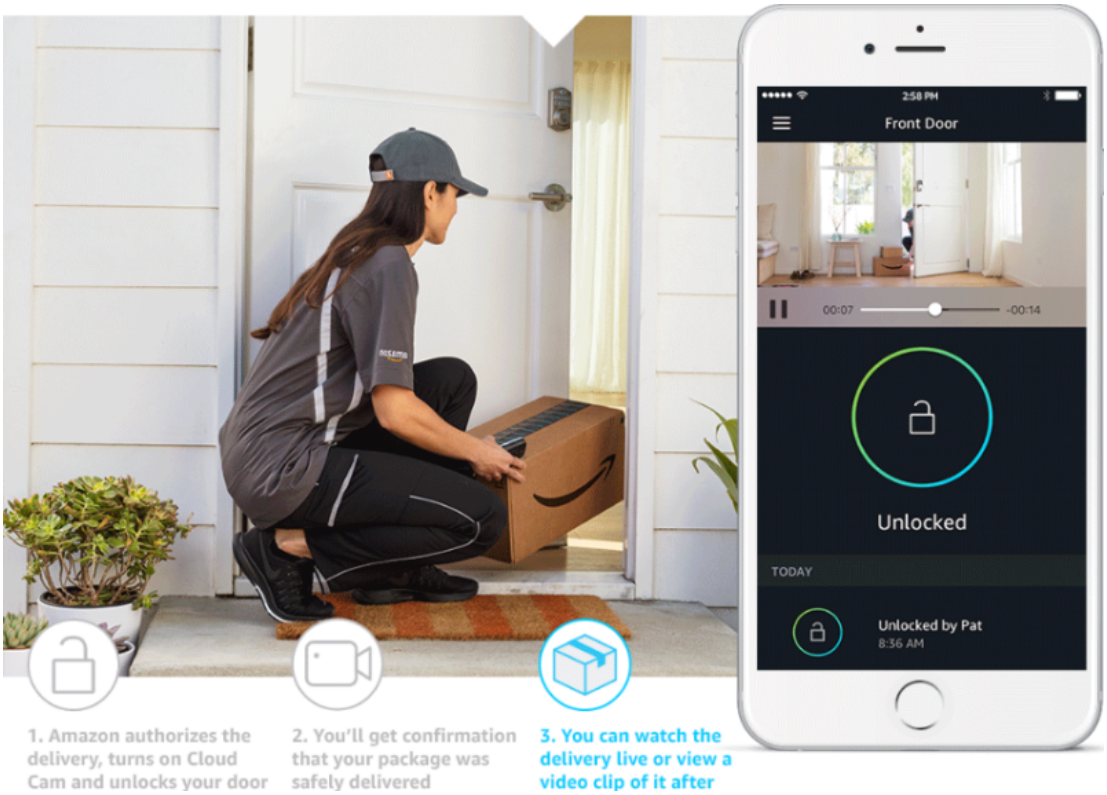
There are two strands to this incident – the company's handling of the breach of 57 million customer and driver records once it found out about it, and the technical failings that allowed it to happen in the first place.

According to Flynn, the hackers were able to access backup files on an Amazon AWS bucket after finding the credentials to access it inside code that had been posted to a weakly-secured GitHub repository. But how had they accessed the repository? Presumably by brute-forcing the password, which was a viable attack method because multi-factor authentication (which GitHub offers in several forms) had not been turned on.

Read More

Even More

Knock, knock. Who's there? Another Amazon Key door-lock hack



The researcher, who's identifying himself only as MG, claimed over the weekend to have found a way to break Amazon Key using a Raspberry Pi equipped with a battery pack and wireless dongle. In a video, he showed himself as a mock hacker, planting the Pi in a hidden location on a doorstep. A fake delivery man then turns up with a package, opens the door using his Amazon Key app and delivers the parcel, before apparently locking the door and leaving. It is, of course, not locked. And the sound of the lock closing is just a fake audio file. When the hacker returns, he's able to just walk right in.

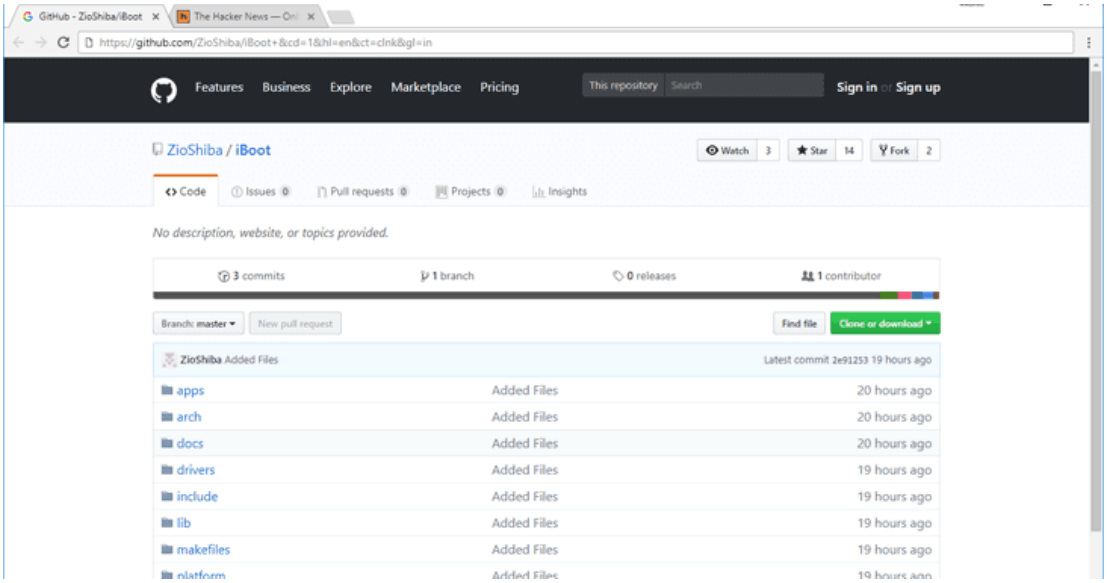
MG won't be releasing the full technical details of the hack until the Key app is patched, though Amazon told Forbes it involved disrupting Wi-Fi connections used by the Key system, not Amazon software. Though MG's video showed an attack involving a driver, it's equally possible his trick could dupe those who use Amazon's lock for everyday use, or permit friends and family to enter with the app. Indeed, MG told Forbes this was a more concerning aspect of his disclosure.

Amazon, in a statement, has downplayed the attack, saying its systems should be able to detect if a door is left unlocked for too long, and that delivery staff should check the front door is locked before leaving.

Read More

Even More

Apple's iBoot Source Code for iPhone Leaked on Github



Apple source code for a core component of iPhone's operating system has purportedly been leaked on GitHub, that could allow hackers and researchers to discover currently unknown zero-day vulnerabilities to develop persistent malware and iPhone jailbreaks. The source code appears to be for iBoot—the critical part of the iOS operating system that's responsible for all security checks and ensures a trusted version of iOS is loaded.

The iBoot code was initially shared online several months back on Reddit, but it just resurfaced today on GitHub (repository now unavailable due to DMCA takedown). Motherboard consulted some security experts who have confirmed the legitimacy of the code.

The leaked source code is being cited as "the biggest leak in history" by Jonathan Levin, the author of a number of books on iOS and macOS internals. He says the leaked code seems to be the real iBoot code as it matches with the code he reverse-engineered himself. It is worth noting that newer iPhones and other iOS devices ship with Secure Enclave, which protects against some of the potential issues that come with the leaked iBoot source code. For now, don't panic. No one's going to hack your iPhone or iPad over the air, nor via a webpage or an app, from this leak.

Read More

Even More

Cutting room floor

- Windows security: Microsoft issues Adobe patch to tackle Flash zero-day
- PoS Malware Steals Credit Card Data via DNS Requests
- Mixpanel analytics accidentally slurped up passwords
- CSS Code Can Be Abused to Collect Sensitive User Data
- Intel Releases New Spectre Patch Update for Skylake Processors
- PSA: If your security starts and ends with bug bounties, you're gonna have a bad time
- How Long is Long Enough? Minimum Password Lengths by the World's Top Sites
- Scammers Use Download Bombs to Freeze Chrome Browsers on Shady Sites
- Vulnerability in spellchecking tool Grammarly
- All Ledger hardware wallets vulnerable to man in the middle attack
- XSS, SQL Injection Flaws Patched in Joomla
- Intel Releases Fixed Skylake Microcodes For Spectre Vulnerability to OEMs

#Tech and #Tools

- usn-search: Facilitate search and processing of .deb packages vulnerabilities and its CVEs.
- DNScrypt Proxy 2.0: A flexible DNS proxy, with support for encrypted DNS protocols.
- CSV Injection in AWS CloudTrail
- Using X.509 certificate as covert channel for data transfer
- Enumerating remote access policies through GPO
- Honey Buckets: Find out who is snooping through your Amazon S3 buckets.
- Stealing CSRF tokens with CSS injection (without iFrames)
- Microsoft Anti Ransomware bypass