Security Newsletter

13 May 2019

Subscribe to this newsletter

Bug in Alpine Linux Docker Image Leaves Root Account Unlocked

A security vulnerability in the Official Docker images based on the Alpine Linux distribution allowed for more than three years logging into the root account using a blank password.

Tracked as CVE-2019-5021, the vulnerability has a critical severity score of 9.8. It was initially reported in build 3.2 of Alpine Linux Docker image and patched in November 2015, with regression tests added to prevent it from occurring in the future. However, a new commit was pushed later that year to simplify the regression tests.

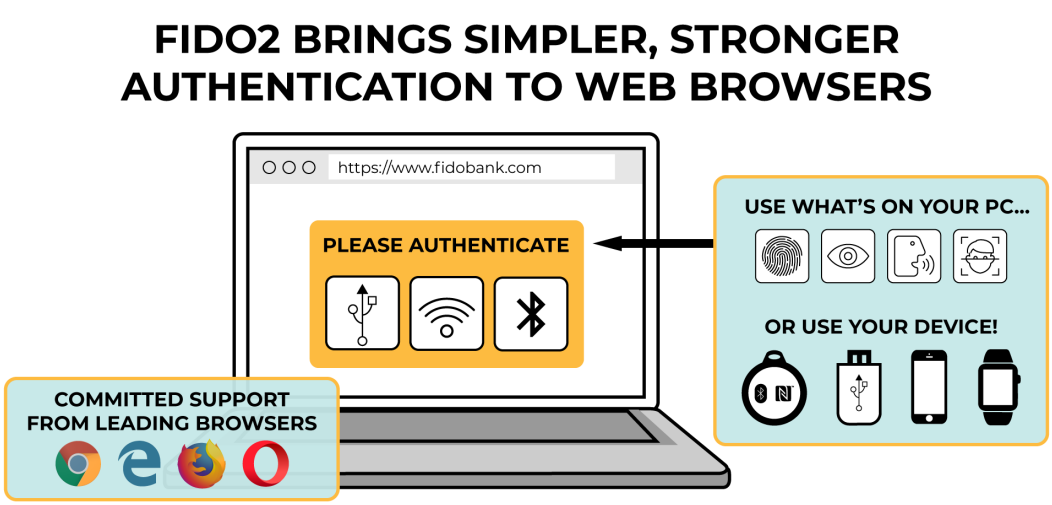
A subsequent commit removed the "disable root by default" flag from the 'edge' build properties file, allowing the bug to regress in the next builds of the image, starting v3.3 to 3.9. The vulnerability was fixed and closed on March 8, 2019, but it could have been solved sooner as it was rediscovered and reported on Agust 5. It slipped through because it was not flagged as a security problem.

To mitigate the issue on systems that still run vulnerable builds of the Alpine Linux container, Cisco Talos recommends disabling the root account.

Read More on BleepingComputer

Even More on SecurityWeek

Windows 10 says Hello to no passwords with FIDO2 certification



Microsoft has passed another milestone on its quest to kill off passwords. The company has now gained official FIDO2 certification for Windows Hello, the Windows 10 biometric authentication system.

The certification applies to Windows 10 version 1903, aka the May 2019 Update, which is scheduled to be released to the public in late May and means Windows Hello has been approved as a FIDO2 'authenticator'. Consumers can expect to start seeing FIDO Certified logos on new Windows 10 PCs, and they'll be able to sign in to online accounts using Windows Hello on all PCs upgraded to version 1903 using the FIDO2 standard.

The certification is part of an industry-wide push for passwordless sign-in, which includes the WebAuthn or Web Authentication WC3 standard that's supported by Mozilla Firefox, Microsoft Edge, and Google Chrome. The standard also has preview support in Apple Safari while Chrome on Android has been officially FIDO2 certificated. The Windows 10 1903 FIDO2 certification extends beyond Microsoft's own software. For example, Windows 10 users who prefer Mozilla Firefox will be able to log into their Microsoft Account and other FIDO-supporting sites with Windows Hello. Additionally, users of Microsoft's Chromium-based Edge will be able to do the same soon.

Read More on ZDNet

More #News

- Researchers' Evil Clippy cloaks malicious Office macros
- CSS tracking trick can monitor your mouse without JavaScript
- Google's Web Packaging standard arises as a new tool for privacy enthusiasts
- Firefox May Add Some Tor Features for Super Private Browsing Mode
- JavaScript Sniffer Attacks: More Online Stores Targeted
- Freedom Mobile leaked millions of card data with CVV codes in plain text
- Burger King's Online Store for Kids Exposes Customers' Info
- Russian cyberspies are using one hell of a clever Microsoft Exchange backdoor
- WordPress 5.2 to Come with Supply-Chain Attack Protection
- Microsoft Windows 10 will get a full built-in Linux Kernel for WSL 2
- NIST Working on Industrial IoT Security Guide for Energy Companies
- Amazon to Disable S3 Path-Style Access Used to Bypass Censorship
- Chinese Hackers Used NSA Hacking Tools Before Shadow Brokers Leaked Them
- Chrome browser pushes SameSite cookie security overhaul
- Six Men Accused of Stealing Over $2.4M in SIM Swapping Attacks
- 275m personal records swiped from exposed MongoDB database
- U.S. Government Details ELECTRICFISH Malware Used by North Korea

#Patch Time!

- Phar Vulnerabilities Patched in Drupal, TYPO3
- Google Patches Remotely Exploitable Vulnerabilities in Android
- Default installation allows user to su to root without password after installing shadow-package

#Tech and #Tools

- "Distroless" Docker Images
- Udica: SELinux security profile generator for containers
- Office365 Attacks
- Evil Clippy: MS Office maldoc assistant
- Deprecating TLSv1.0 and TLSv1.1 gracefully with Cloudflare Workers
- Exploiting 10K+ devices used by britain's most vulnerable
- Exploring Mimikatz - Part 1 - WDigest
- Queue the Hardening Enhancements
- SSH Honey Keys
- Why You Shouldn't Use a Password Manager For Your Linode Account

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us