Security Newsletter
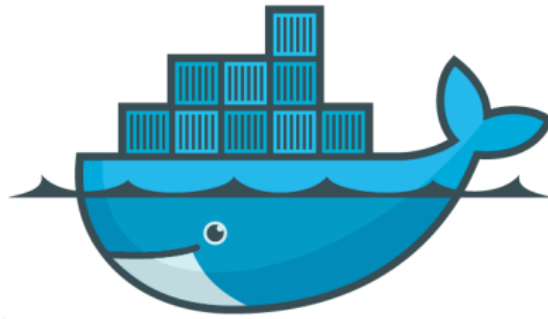
6 May 2019

Docker breach of 190,000 users exposes lack of two-factor authentication

Docker Hub, one of the largest cloud-based library of Docker container images, has suffered a data breach after an unknown attacker gained access to the company's single Hub database. Docker Hub is an online repository service where users and partners can create, test, store and distribute Docker container images, both publicly and privately.

According to an advisory on the company's website, the incident happened on 25 April when for a "brief period" attackers accessed a single Docker Hub repository used to store the accounts. Exposed data included usernames, an unknown number of hashed passwords and, inconveniently, API tokens used by developers with GitHub and Bitbucket (which, when embedded in scripts, perform the same function as passwords for Docker autobuilds).

Data breaches are always bad news but the possible compromise of 190,000 accounts (about 5% of the service's user base) on a development system used by businesses heaps additional worries on top of the usual workload. And that's what makes the Docker Hub breach potentially so much more worrying: If tokens have been compromised, it gives attackers many more places to slip in malicious code.

Read More on Naked Security blog

Even more on The Hacker News

Docker Hub Breach: It's Not the Numbers; It's the Reach

More #News

- Magecart Group 12 Targets OpenCart Websites
- WikiLeaks' Assange Signals He'll Fight Extradition to US

- Is a sticky label the answer to the IoT's security problems?
- Google rolling out auto-delete for your location and activity history
- On Security Tokens
- Coinhive Dead but Browser-Based Cryptomining Still a Threat
- Data: E-Retail Hacks More Lucrative Than Ever
- Hackers lurked in Citrix systems for six months
- Security Recruiter Directory
- Microsoft 365 Adds More Control Over Encrypted Emails, Increases Privacy
- Unprotected Database Exposes Personal Info of 80 Million American Households
- Mozilla To Disable Firefox Add-Ons with Obfuscated Code
- Over Dozen Popular Email Clients Found Vulnerable to Signature Spoofing Attacks
- Scammers Create Google Search Ads to Lure PayPal, Amazon Clients
- 60 percent of enterprise codebases contain open-source vulnerabilities

#Patch Time!

- Pre-Installed Software Flaw Exposes Most Dell Computers to Remote Hacking
- 50,000 enterprise firms running SAP software vulnerable to attack
- Cisco Patches Critical Vulnerability in Data Center Switches
- Alerts: Vulnerability in Philips Records System
- Recent Oracle WebLogic zero-day used to infect servers with ransomware
- Over two million IoT devices vulnerable because of P2P component flaws
- Vulnerable Confluence Servers Get Infected with Ransomware, Trojans
- Cisco Finds Serious Flaws in Sierra Wireless AirLink Devices
- Critical Unpatched Flaw Disclosed in WordPress WooCommerce Extension

#Tech and #Tools

- Open Source SIRP with Elasticsearch and TheHive - Overview
- How to reverse malware on MacOS without getting infected | part 1
- Story of a Hundred Vulnerable Jenkins Plugins
- Remote Code Execution on most Dell computers
- Azure Security Logging – part 2: security-logging capabilities of Azure resources
- ASecure.Cloud: free repository of customizable AWS security configurations and best practices
- A few Ghidra tips for IDA users, part 3 - conversion, labels, and comments
- AWS IAM exploitation techniques
- AutoMacTC: Automating Mac Forensic Triage
- XSS-Auditor — the protector of unprotected
- Red Team Supply Chain Attacks in Modern Software Development Environments
- Windows NamedPipes 101 + Privilege Escalation

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