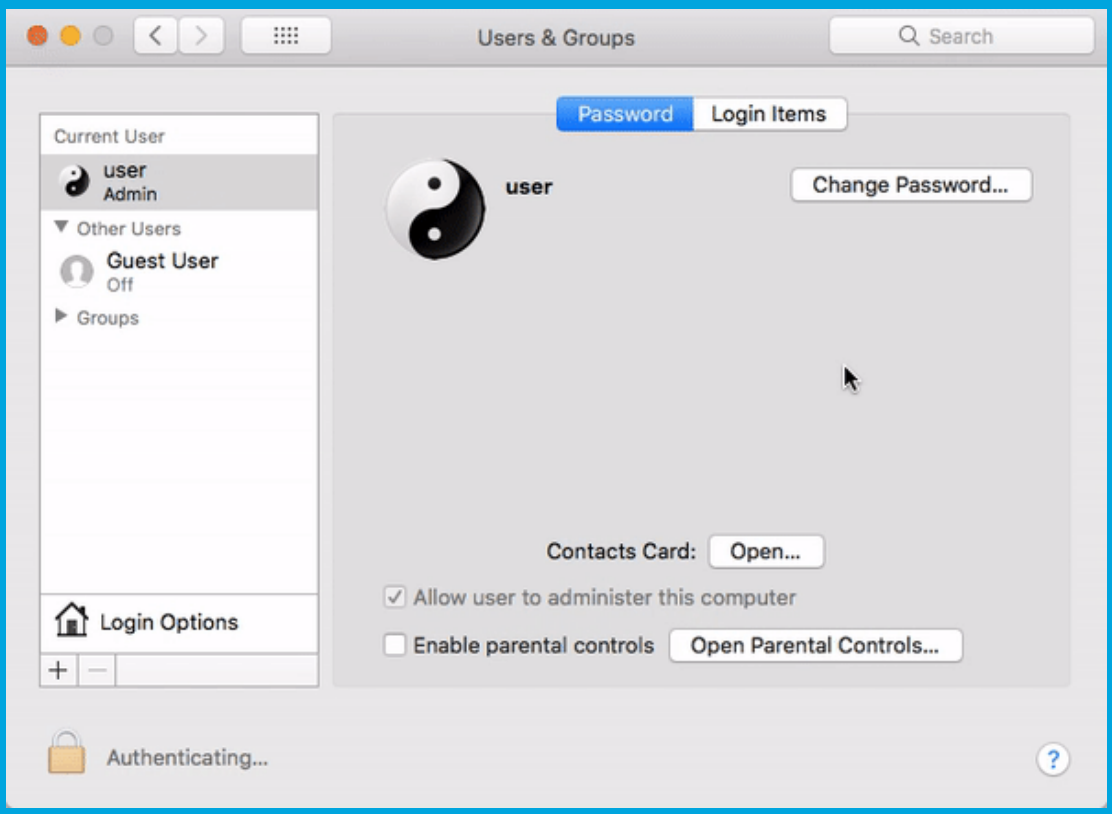
Security Newsletter

04 December 2017

Subscribe to this newsletter

MacOS High Sierra Bug: Change Root Password Now or Patch



A newly-discovered flaw in macOS High Sierra allows anyone with local (and, apparently in some cases, remote) access to the machine to log in as the all-powerful "root" user without supplying a password. Fortunately, there is a simple fix for this until Apple patches this inexplicable bug: Change the root account's password now.

High Sierra users should be able to replicate the exploit by accessing System Preferences, then Users & Groups, and then click the lock to make changes. Type "root" with no password, and simply try that several times until the system relents and lets you in.

How does one change the root password? Open up a Terminal (in the Spotlight search box just type "terminal") and type "sudo passwd root". Sources who have tested the bug say it can be exploited remotely if a High Sierra user has enabled "screen sharing" on their Mac. Likewise, multiple sources have now confirmed that disabling the root account does not fix the problem because the exploit actually causes the account to be re-enabled.

Apple has released a patch, but this patch appears to break the operating system's file sharing functionality in some cases. The company has provided an easy fix for affected users. Users simply need to open the Terminal, type the command *sudo /usr/libexec/configureLocalKDC*. This addresses the issue until Apple releases another update.

This is not the only authentication bug found in macOS High Sierra recently. Last month, a developer noticed that the operating system had leaked the passwords for encrypted Apple File System (APFS) volumes via the password hint.

Read More

Why "blank" Gets You Root (Technical)

US Army and NSA Files Left Exposed Online on Amazon S3 Server

Ten days after an Amazon S3 server exposed data from the US Army's CENTCOM and PACOM divisions, security researchers have identified another S3 server instance that leaked files from INSCOM, a joint US Army and NSA agency tasked with conducting intelligence, security, and information operations.

Of these three, researchers said that one was an Oracle Virtual Appliance (.ova) file that was an image of a virtual machine running a Linux-based operating system and an attached virtual hard drive. Researchers were not able to boot the OS or access any of the files stored on the virtual hard drive. Nonetheless, the metadata of files stored on the virtual hard drive allowed researchers to determine the SSD image held troves of highly sensitive files.

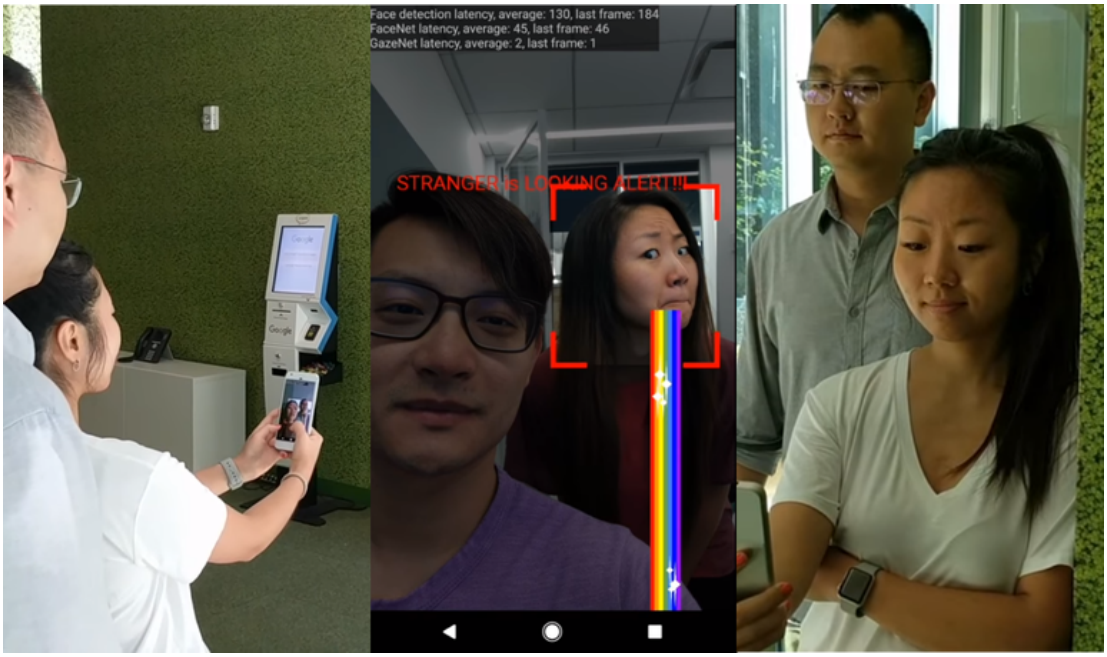
In addition, a folder in the same VM image also indicated that the system was also part of Red Disk, a cloud computing platform that was part of the Distributed Common Ground System-Army (DCGS-A), a "battlefield intelligence platform" developed by the DOD. Early tests showed the platform was incredibly slow, and mostly hindered existing operations. The project never made it out of the testing stage, and the DOD eventually scraped it in 2014.

Regrettably, this cloud leak was entirely avoidable, the likely result of process errors within an IT environment that lacked the procedures needed. That being said, It was an intelligence distribution system under development, not raw intelligence. The researcher that discovered the data, didn't disclosed anything.

Read More

NSA "Red Disk" Data Leak

Snoopers beware: Google's AI can now spot shoulder-surfers peeking at your screen



Google researchers have developed a privacy application that can instantly detect when a stranger glances at your screen over your shoulder. When the user holds a phone up to chat or view a private video, say, on a train or other crowded place, the algorithm will detect when someone else from behind begins looking at the screen too. The video shows that the algorithm can detect a stranger's gaze within milliseconds.

The video suggests the researchers are using FaceNet, a facial-recognition neural network developed by Schroff and other Google researchers in 2015, as well as GazeNet, a gaze-estimation neural network recently described by researchers in Japan and Germany. The two Google researchers call their application an 'electronic screen protector', which combines the two areas of computer vision research to provide enhanced privacy when using a big-screen smartphone in public spaces.

Researchers See Jung Ryu and Florian Schroff will demonstrate their shoulder-surfing warning system at next month's Neural Information Processing Systems Conference in California.

Read More

Demo video

Keybase Bug Might Have Backed up Your Private Encryption Key on Google's Servers

Keybase is notifying Android users of a bug in its mobile app that might have unintentionally included the users' private key —used to encrypt conversations and other private data— into the automatic backups created by the Android OS and uploaded on Google's servers.

Keybase, which is a company that provides a wide range of identity proofing and encrypted communication tools, says it fixed the bug and has sent notification emails to users it believes are affected by this issue. According to an email seen by Bleeping Computer, the issue appears to affect only "early adopters" of the Keybase Android app.

An attacker may obtain a user's Keybase account password (passphrase), but he won't be able to impersonate that user in Keybase-encrypted chats and private PGP-protected messages unless he sends those messages from verified devices. The bug Keybase just fixed allows an attacker to obtain the private key and impersonate the user's Android smartphone. This is why it is important that users secure devices, even if there's a little possibility they were affected.

Despite this issue, users shouldn't be deterred from using Keybase, which is currently the only service that provides support for end-to-end encrypting Git operations, Reddit and Twitter private messages.

Read More

Several Vulnerabilities Patched in PowerDNS

Updates released for the authoritative nameserver and recursive nameserver components of PowerDNS patch several vulnerabilities that can be exploited for denial-of-service (DoS) attacks, records manipulation, modifying configurations, and cross-site scripting (XSS) attacks.

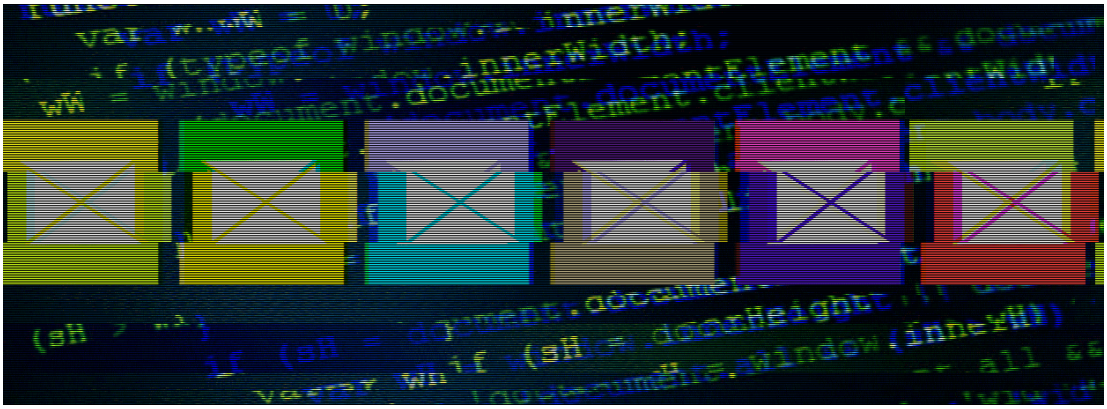
None of the bugs pose a risk that PowerDNS might itself be compromised, but this is the DNS: what an attacker can do is fool around with DNS records in various ways. That can be catastrophic if done right: for example, if a network is tricked into advertising itself as the whole of the Internet, it can be hosed, or if the wrong network promises it's the best way to reach YouTube, then YouTube is blackholed.

PowerDNS's Remi Gacogne told the OSS-Sec mailing list the bugs affect only non-default configurations, and noted that users on the version 3 stream can download "minimal" patches.

Read More

Even More

No Patch Available for RCE Bug Affecting Half of the Internet's Email Servers



A critical remote code execution flaw affects over half of the Internet's email servers, and there's no fix for it available, just yet. The bug is a vulnerability in Exim, a mail transfer agent (MTA), which is software that runs on email servers and that relays emails from senders to recipients.

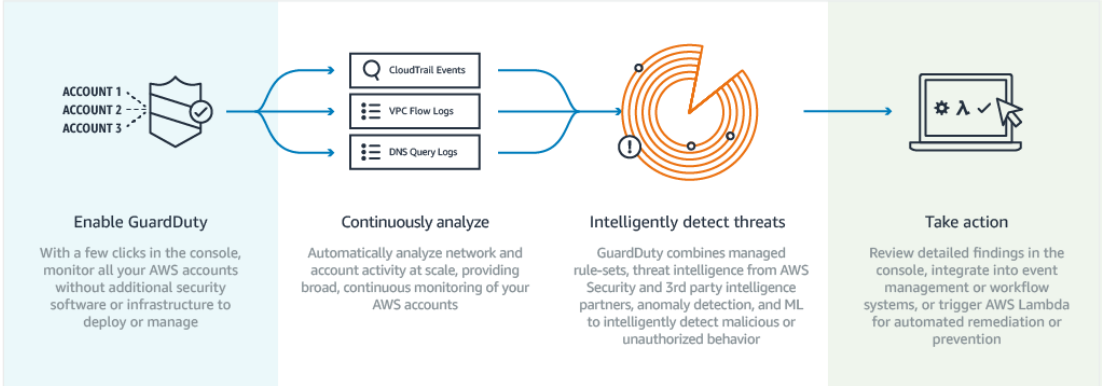
According to a security alert published last week on Exim's website, the Exim development team was notified of two bugs that impact Exim 4.88 and 4.89, the two latest Exim versions. The most dangerous of the two bugs is the one tracked as CVE-2017-16943, which is a use-after-free vulnerability that leads to remote code execution on affected servers.

The Taiwanese researcher who discovered the bug published his findings, including proof-of-concept code, on Exim's public bug tracker. The researcher said the Exim team did not list an email address for reporting security flaws in private, a mistake that the Exim team admitted.

"A tentative patch exists but has not yet been confirmed," said Phil Pennock, one of the Exim developers, in a security alert published late last week. A workaround is available in the article.

Read More

Amazon adds security monitoring and threat defence with GuardDuty



Amazon has launched GuardDuty, a new intelligence-driven threat detection service that uses machine learning to locate anomalies and notify the user when it finds something suspect.

The new offering scans public and AWS-generated events looking for trends, patterns, and anomalies. Findings of the scans are presented to the user as one of low, medium, or high level, along with evidence and recommendations for remediation.

GuardDuty consumes multiple data streams, including several threat intelligence feeds, staying aware of IP addresses and domains flagged as malicious, while also learning to identify malicious or unauthorised behaviour in a user's AWS account. GuardDuty runs completely on AWS infrastructure, with no agent or sensor to install, or even a network appliance required to run it.

Read More

AWS product page

Cutting room floor

- New web browsing security tool arrives: DNS over TLS
- Wondering why your internal .dev web app has stopped working?
- Don't shame idiots about their idiotically weak passwords
- RepoSsessed: parse public source code repositories and find various types of vulnerabilities.
- "Huge Dirty COW" (CVE-2017–1000405): The Incomplete Dirty COW patch
- Even Highly Skilled Cyber-Thieves Make Stupid Mistakes, or Do They?
- Cryptocurrency Wallet Apps Are a Security Disaster Waiting to Happen
- Persistent drive-by cryptomining coming to a browser near you
- Here's What I'm Telling US Congress about Data Breaches
- Tiredful API: Damn insecure REST API
- The art of fuzzing: Slides and demos
- SWORD dropbox: A $15 OpenWRT based DIY disposable pen-test tool.
- Using DNS to break out of isolated networks in a AWS cloud environment
- Exploring cmdkey: An Edge Case for Privilege Escalation
- Unofficial Guide to Mimikatz and Command Reference
- Symantec Encryption Desktop Local Privilege Escalation – Exploiting an Arbitrary Hard Disk Read/Write Vulnerability Over NTFS

Kindred Group in brief

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