Erledigt High Sierra Sicherheitslücke root Zugriff

Beitrag von „hitman20“ vom 29. November 2017, 02:48

Hallo,

ich habe gerade auf Twitter und auf giga.de gefunden, das Apple vergessen hat unter High Sierra den root User zu schützen bzw. ein Passwort dafür zu geben. Man kann dann zum Beispiel in den Systemeinstellungen unter Benutzer und Gruppen auf das Schloss klicken und dort den Benutzer root eingeben ohne Passwort und die Authentifizierung muss dan zwei mal bestätigt werden, und man ist dann als root User angemeldet. Im Menüpunkt Sicherheit in den Systemeinstellungen funktioniert es dann zum Beispiel auch. Apple arbeitet wohl schon an einem Fix. Am besten ist es dann, wenn Ihr dem root User dann ein sicheres Passwort vergebt. Ein neues Passwort für den root User kann man im Terminal mit dem Befehl "sudo passwd" vergeben. Dort müsst Ihr einmal euer eigenes Passwort eingeben und dann könnt Ihr das neue root Passwort eingeben, das man zwei mal bestätigen muss. Ich konnte das bei mir nachstellen unter 10.13.1.

Die Links dazu sind http://www.giga.de/downloads/m...wort-vorlaeufige-loesung/ und https://twitter.com/lemiorhan/status/935578694541770752

Falls das doch schon gepostet wurde, bitte löschen.

Gruß

hitman20

Beitrag von „al6042“ vom 29. November 2017, 07:15

Nope... ist passend und frisch...
Ich habe das eben mal versucht nachzustellen, aber nach zweimal 20 Versuchen bleiben

lassen.
Bin aber trotzdem gespannt auf das Update und wann es tatsächlich auftauchen soll.

Beitrag von „a1k0n“ vom 29. November 2017, 07:38

Etwas Offtopic aber trotzdem ratsam. Giga.de finanziert sich jetzt durch unschöne Machenschaften. Habe vorigen Monat die Seite per 4G angesteuert weil es ganz oben stand in der Googlesuche da poppte das übliche "wollen sie die Seite in der Mobilen Ansicht oder Desktop Version lesen" Fenster auf. 4,99€ kam der Spass. Und es gab keine weg zurück.

Beitrag von „Shado“ vom 29. November 2017, 08:19

Das ist natürlich eine große Schlappe von den Programmierern. Oder ist das so gewollt????


Beitrag von „jboeren“ vom 29. November 2017, 09:12

alu hut modus Das ist so gewollt!

Beitrag von „Dr.Stein“ vom 29. November 2017, 10:10

Money Money Money .... wer weiß ob da was dran ist

Beitrag von „umax1980“ vom 29. November 2017, 10:14

Das ist nur für die Nutzer die schnell mal ihr Kennwort vergessen, damit sie nicht so einen Schreck bekommen.
Das Apple das nicht als Feature für 9,99 Euro anbietet....

Beitrag von „grt“ vom 29. November 2017, 11:05

aber ich hab noch kein highSierra.. 

Beitrag von „umax1980“ vom 29. November 2017, 11:07

Dann darfst du dein Kennwort nicht vergessen ....

Beitrag von „grt“ vom 29. November 2017, 11:10

@umax1980 nö - das hab ich dick und fett mit dem edding auf den monitor gemalt.
interessant wär ja, ob eine anmeldung als root - ohne passwort - funktionieren würde. ubuntu hat ja auch einen passwortbefreiten root, aber der hat keine chance, sich irgendwiewo anzumelden.

Beitrag von „umax1980“ vom 29. November 2017, 11:17

Das werd ich gleich mal probieren....
Diese Edding-Methode ist aber nur optimal wenn du abwischbaren Edding nutzt. Außer du änderst das nicht mehr ab.

Beitrag von „grt“ vom 29. November 2017, 11:46

> Zitat von umax1980
>
> abwischbaren Edding

nicht katzenkompatibel.. ist halt ein dauerfixiertes passwort.

aber im ernst - mich juckt es grad mächtig in den fingern: was ginge da denn alles mit einem freiherumwuselnden root ohne passwort? da muss ich wohl doch entgegen alle meine spielregeln eine version vor xx.xx.5/6/7 installieren.

und überhaupt - wie passiert sowas? high sierra wird doch nicht von grund auf neu entwickelt (da könnte ich noch verstehen, dass man den root einfach vergisst abzusichern) - in den vorherigen osx-versionen gibts die lücke nicht
ich muss mir wohl schnellstmöglich einen aluhut besorgen.... (bzw. einen für den rechner)

Beitrag von „umax1980“ vom 29. November 2017, 11:51

Eigentlich unglaublich diese Sache.
Irgendwie kommt jeden Tag was neues, bei dem man denkt, daß kann doch nicht angehen.

Beitrag von „Sascha_77“ vom 29. November 2017, 12:18

Allerdings. Damit haben die so ziemlich den Vogel abgeschossen. Wenns beim normalen Nutzer (ohne Adminrechte) so wäre dann wäre das auch schon schlimm. Aber gleich der Root? Respekt.

Beitrag von „grt“ vom 29. November 2017, 13:55

> Zitat von Sascha_77
>
> Wenns beim normalen Nutzer (ohne Adminrechte) so wäre

bei dem (elCapitan) konnte man noch nicht mal programme installieren, oder schlösser aufmachen, wenn der "normale" user - zwar als admin deklariert - kein passwort hatte - wie das allerdings funktioniert, adminuser ohne passwort anzulegen hab ich nicht rausgekriegt.

Beitrag von „umax1980“ vom 29. November 2017, 14:43

Das funktioniert tatsächlich - User root eintragen, dreimal Enter, es können auch 4 Mal gewesen sein. Schloss ist offen.
Ich werde da jetzt nichts weiter verstellen, aber dem root ein Passwort geben.

Da sollte Apple aber schleunigst einen Patch bringen !!!

Beitrag von „yoyo268“ vom 29. November 2017, 14:50

Hallo Sascha_77!
Naja, wie heißt es so schön: entweder Ganz oder Garnicht

Schönen Gruß!

Beitrag von „Schorse“ vom 29. November 2017, 14:54

Moin,
Jepp, klappt prima... Das schlimme daran ist das die Info nun öffentlich bekannt ist. Da macht sich doch jetzt jeder kleine Häcker auf den Weg... Unfassbar Apple

---

Beitrag von „Si Vis Pacem“ vom 29. November 2017, 15:20

Einfach Folgendes eingeben. Dann zuerst das User-Passwort und dann das zukünftige root-Passwort.

Code

1. sudo passwd

Beitrag von „Dr.Stein“ vom 29. November 2017, 15:29

Eben bei MediaMarkt ein paar Passwörter getauscht .. 

Beitrag von „Higgins12“ vom 29. November 2017, 15:31

Du schlimmer Finger du

Beitrag von „umax1980“ vom 29. November 2017, 15:35

Jetzt mal freundlich auf die Möglichkeit hinweisen das du das wieder zurück setzt.
Im Gegenzug Warengutscheine.

Beitrag von „Nichticke“ vom 29. November 2017, 15:39

@Dr.Stein genau daran habe ich auch gedacht nur halt direkt im Applestore. Oder bei Saturn die mir kein AppleTV verkaufen wollten.

Beitrag von „Sascha_77“ vom 29. November 2017, 15:42

Coole Aktion.

Beitrag von „Dr.Stein“ vom 29. November 2017, 15:50

Naja ich hab ja über all einen Hinweis hinterlassen

Beitrag von „Schorse“ vom 29. November 2017, 15:57

Moin,
durch die Spielerei habe ich nun einen weitern Benutzer "Andere Benutzer"
beim deaktivieren kommt die Meldung!

"It is not possible to turn off the Other... option when the root user is turned on."

Und nu?

Beitrag von „Dr.Stein“ vom 29. November 2017, 16:21

Bist du als Admin angemeldet ?

Beitrag von „Schorse“ vom 29. November 2017, 16:28

Okay.. kann mit der App "Directory Utility" wieder deaktiviert werden.

Beitrag von „apfelnico“ vom 29. November 2017, 16:32

Gehe zu Systemeinstellungen -> Benutzer & Gruppen -> Anmeldeoptionen -> Netzwerkaccount-Server: Verbinden –> Verzeichnisdienste öffnen -> Zum Bearbeiten auf das Schloss klicken.

Im Bearbeiten-Menü findest du "root-Benutzer deaktivieren"

Geht natürlich auch via Terminal ...

Beitrag von „hitman20“ vom 29. November 2017, 16:47

Im Terminal reicht es, wenn man den Befehl eingibt, um den root Benutzer zu deaktivieren: dsenableroot -d.

Beitrag von „lahu“ vom 29. November 2017, 17:22

Sicherheitsupdate....
soeben geladen und installiert

Beitrag von „Higgins12“ vom 29. November 2017, 17:41

Na das nenn ich mal wieder fix von Apple. M$ hätte da Monate für gebraucht.

Beitrag von „al6042“ vom 29. November 2017, 18:34

Eben ohne Neustart auf allen Geräten erfolgreich installiert.
Das war jetzt schon sowas wie fix, würde ich sagen...

EDIT:

Achtung... die Build Nummer wird durch das Update verändert.
Es wird dann die Nummer 17B1002 angezeigt.

Für Nvidia WebDriver-User heisst, dass:
Ohne Vorarbeit, wird unter Umständen der Rechner nicht mehr komplett hochfahren, da die WebDriver auf das vorherige Build eingeschossen sind.

Abhilfe:
Als Abhilfe habe ich vor dem Neustart das Tool Nvidia Webtreiber all Version update App für High Sierra ausgeführt.

Ergebnis:
Läuft wie es soll...

EDIT 2:

Nach dem Neustart funktioniert der Zugriff auf Datei-/Ordner-Freigaben nicht mehr.
Das Anmeldefenster erscheint, aber die Credentials werden nicht angenommen.

EDIT 3:

Damit die Datei-/Ordner-Freigaben wieder funktioniert, muss in den "Option" unter "System Preferences"->"Sharing"->File Sharing" nun auch der User explizit zugeordnet und besätigt werden.
Danach geht es wieder...

Beitrag von „umax1980“ vom 29. November 2017, 19:16

Eins muss man Apple lassen, fix reagiert.

Beitrag von „grt“ vom 29. November 2017, 19:20

@Dr.Stein sowas aber auch.. 

Beitrag von „Schorse“ vom 29. November 2017, 19:41

@al6042 fettes Danke...
Jawoll, das nenne ich mal flott von Apple, schnell reagiert!
Auch die rasche Lösung hier im Forum für Nvidianutzer.
Sagenhaft

Beitrag von „al6042“ vom 29. November 2017, 20:38

An der Stelle nochmal ein riesengroßes Danke schön an @G4_Hacker, für dieses geniale WebDriver-Tool...

Beitrag von „ductator“ vom 29. November 2017, 21:48

Und https://support.apple.com/en-us/HT208315 die Apple Support Seite zum Fix.
Man beachte vor allem den letzten Hinweis, falls man dem Root Nutzer braucht.

Beitrag von „FairLight“ vom 30. November 2017, 00:13

Was macht man wenn man erst das Update gemacht hat und will dann die Nvidia Treiber installieren?

Beitrag von „griven“ vom 30. November 2017, 00:20

Mit nv_disable=1 als boot-arg starten oder alternativ bei Clover die Space Taste drücken im boot Menu und da dann Force Vesa for NVIDIA oder so ähnlich auswählen (ich weiß nicht aus dem Kopf wie der Eintrag genau heist aber NVIDIA und VESA kommen vor) und dann boot with selected options wählen und anschließend den Treiber installieren bzw. Updaten

---

Beitrag von „FairLight“ vom 30. November 2017, 00:37

Das habe ich gemacht.
Dann kommt aber immer noch die Meldung:

Mac OS X version 10.13.1 (17B1002) is not supported with this package. Please see NVIDIA’s website for further driver information.

Beitrag von „griven“ vom 30. November 2017, 00:42

Logisch gibt ja auch für diese Build Version noch keine aber das hier schafft Abhilfe: Nvidia Webtreiber all Version update App für High Sierra

---

Beitrag von „FairLight“ vom 30. November 2017, 00:45

Nvidia Webtreiber all Version update App für High Sierra meldet:

NVDAStartupWeb.kext nicht gefunden.
Bitte prüfen ob der Webtreiber installiert wurde!

Ich denke mal es muss erst Nvidia Web Treiber installiert sein um es zu patchen.

Beitrag von „griven“ vom 30. November 2017, 01:10

Logisch muss das so sein, hast Du noch keinen installiert dann ist das hier das richtige für Dich: NVIDIA® WebDriver Updater.app

---

Beitrag von „motiongroup“ vom 30. November 2017, 05:47

https://9to5mac.com/2017/11/29/how-to-fix-macos-file-share/

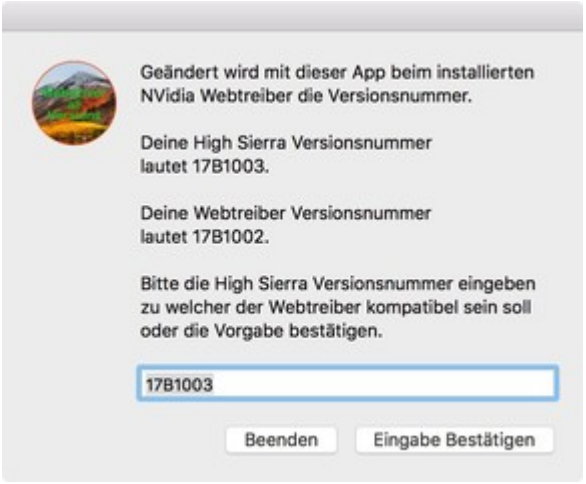
das perlt aber aber so richtig

Beitrag von „Futzi“ vom 30. November 2017, 06:43

Wurde nochmal nach gepatcht sind jetzt bei version 17B1003

Beitrag von „al6042“ vom 30. November 2017, 08:01

Danke für die Info...
Habe den oben beschriebenen Vorgang auch gleich wiederholt:



Beitrag von „macmac512“ vom 30. November 2017, 09:34

> Zitat von Higgins12
>
> Na das nenn ich mal wieder fix von Apple. M$ hätte da Monate für gebraucht.

> Zitat von al6042
>
> Eben ohne Neustart auf allen Geräten erfolgreich installiert.
> Das war jetzt schon sowas wie fix, würde ich sagen...

> Zitat von umax1980
>
> Eins muss man Apple lassen, fix reagiert.

https://forums.developer.apple.com/thread/79235#277225

Über zwei Wochen Root ohne Passwort zu lassen ist fix? naja.... 

Das ist alles aber eben nicht fix. nur ohne große Publicity funktioniert bei Apple leider gar nichts.

Beitrag von „Nightflyer“ vom 30. November 2017, 10:43

Wieso bekomme ich das Update zweimal?
Einmal letzte Nacht installiert und eben war es wieder da

Beitrag von „Higgins12“ vom 30. November 2017, 10:45

Update fürs Update  .. hatte ich auch.

Beitrag von „Harper Lewis“ vom 30. November 2017, 10:55

Das Update wird jetzt übrigens automatisch ausgeführt, wenn man es noch nicht selbst angeworfen hat. Das habe ich zumindest gelesen...

Beitrag von „Dr.Stein“ vom 30. November 2017, 11:03

bis jetzt hatte ich nur 1 Update
seid dem kann ich mich nicht mehr als root User einloggen

Beitrag von „Sascha_77“ vom 30. November 2017, 11:07

Guckst du hier:

https://support.apple.com/en-us/HT204012

Beitrag von „Dr.Stein“ vom 30. November 2017, 11:10

Ich wollte damit sagen das dieses Update gewirkt hat

Beitrag von „Thogg Niatiz“ vom 30. November 2017, 13:21

@al6042 woran könnte es liegen, dass der Webdriver Patch nicht komplett funktioniert? Ich habe seit ein paar Tagen zum ersten mal eine Geforce Grafik (960) im Einsatz und jetzt zum ersten Mal Ärger mit den Treibern. Ohne Patch meldet sich der Nvidia Driver Manager zu Wort, dass die Apple Treiber wegen Inkompatibilität des Webdrivers geladen wurden. Mit Patch werden angeblich die Webdriver verwendet, aber von QE/CI sehe ich hier nichts...

Beitrag von „Futzi“ vom 30. November 2017, 14:05

Hatte das selbe problem mit einem

Code

1. sudo kextcache -i /

war der webdriver nach einem neustart wieder da

Beitrag von „Thogg Niatiz“ vom 30. November 2017, 14:52

Normalerweise übernimmt der Patcher von G4_Hacker das. Aber dank deines Hinweises bin ich drauf gekommen, dass genau dieser Vorgang fehlgeschlagen ist (schade, dass der Patcher selbst keine Debugausgabe bietet), weil meine SIP komplett aktiv war. Jetzt habe ich mit der csractiveconfig=0x0001 unsignierte Kexts erlaubt und seitdem funktioniert es.

Beitrag von „Chrisv6“ vom 30. November 2017, 19:12

Hallo, bei mir geht das nicht, wo gebe ich csractiveconfig=0x0001 ein? Hab es als bootleg versucht kommt dennoch:

Untrusted kexts are not allowed

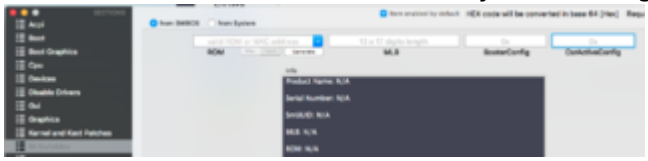
Kext with invalid signature (-67030) denied: /Library/StagedExtensions/Library/Extensions/69E7386E-E94C-4E3A-A6D5-58005EC713B3.kext

Bundle (/Library/Extensions/NVDAStartupWeb.kext) failed to validate, deleting: /Library/StagedExtensions/Library/Extensions/69E7386E-E94C-4E3A-A6D5-58005EC713B3.kext

---

Beitrag von „Thogg Niatiz“ vom 30. November 2017, 19:30

Entweder in der Clover GUI in der System Konfiguration oder im Clover Configurator



Beitrag von „Chrisv6“ vom 30. November 2017, 19:40

Ok. Danke Jz gehts... LG

Beitrag von „al6042“ vom 30. November 2017, 21:14

@Thogg Niatiz
Bei mir hat der Patcher alles richtig gemacht... Info.plist geändert und danach auch die Rechte wieder sauber gesetzt...
Auf den Cache habe ich nicht geachtet...

Beitrag von „FairLight“ vom 30. November 2017, 23:05

@griven Danke das hat funktioniert.

Beitrag von „griven“ vom 30. November 2017, 23:08

So soll es doch sein

Beitrag von „Schorse“ vom 3. Dezember 2017, 00:40

Moin!
Kann das jemand bestätigen? Oder ist heute der 1 April?

Lächerlich: Neuestes macOS Update macht Root-Bug-Fix rückgängig
https://www.apfellike.com/2017...oot-bug-fix-rueckgaengig/

Beitrag von „Dr.Stein“ vom 3. Dezember 2017, 00:41

LOL... wie dämlich ..

Beitrag von „MacGrummel“ vom 3. Dezember 2017, 04:13

Kann ich bestätigen. Ist aber eigentlich auch logisch, weil nicht im schon älteren Update enthalten muss es nochmal nachinstalliert werden.. Die Beta- und Public-Beta-Tester haben den Fix dann erst nen Tag später mit 10.13.2 beta 6 gleich mit installiert bekommen, da gab es im ersten Schub keine passende Version..