

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur

Manual

Howard Oakley <https://eclecticlight.co>

In 2016, some brand new MacBook Pros shipped to users with one of the key parts of their security protection – System Integrity Protection, or SIP – turned off. It wasn't until they were updated to macOS Sierra 10.12.2 some weeks later that this was turned back on, and they benefitted from the protection from malware that they require.

When I first heard about this, it occurred to me that users cannot easily check whether any of the powerful protection systems built into macOS have become disabled, or their protection data files (which are normally updated silently by Apple) had become out of date.

LockRattler lets you check these most important and otherwise hidden features in macOS without having to type magical incantations into Terminal. I hope that it will provide you with assurance, or at least will enable you to fix a problem before any malware does.


What you need

- A Mac running macOS El Capitan, Sierra, High Sierra, Mojave, Catalina or Big Sur.
- A copy of the latest version of LockRattler from [The Eclectic Light Company](https://eclecticlight.co) (This is delivered by secure HTTPS download.)

Getting started

LockRattler comes compressed as a Zip file, which you should decompress, and move the app to your preferred folder, such as /Applications. It is not fussy where it is run from, though.

LockRattler is now not just properly signed, but is also notarized. If the app doesn't open correctly when you first try to run it, please contact me immediately.

 Each time LockRattler runs, it checks its contents against its code signature. If it finds a discrepancy, it quits immediately but doesn't crash. If that happens when you try to run the app, first replace it with a fresh copy, in case the app has simply become corrupted. You may also wish to check for disk problems, and rule out the presence of malware, which could be responsible.

Although LockRattler accesses important information in your Mac, it doesn't need to access any from the special areas protected by Mojave's new privacy system. You don't need to give it any special access rights in the **Security & Privacy** pane. If you're unsure what settings to use, look at the explanation in the **Privacy settings** command in the **Help** menu.

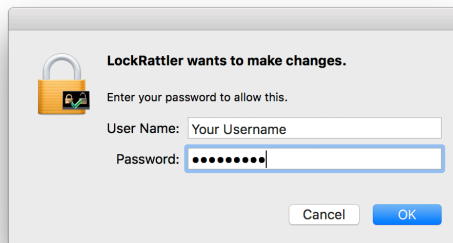
To run the app, simply double-click it, or open it in any of the other normal ways. It then displays its only window. When you close that window, Lock Rattler automatically quits.

When that window first opens, it runs all its tests except that for three, **Software update**, **Log private data** and **Firmware password**, and doesn't perform any of the three checks for updates available lower down.

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur Manual

Howard Oakley <https://eclecticlight.co>

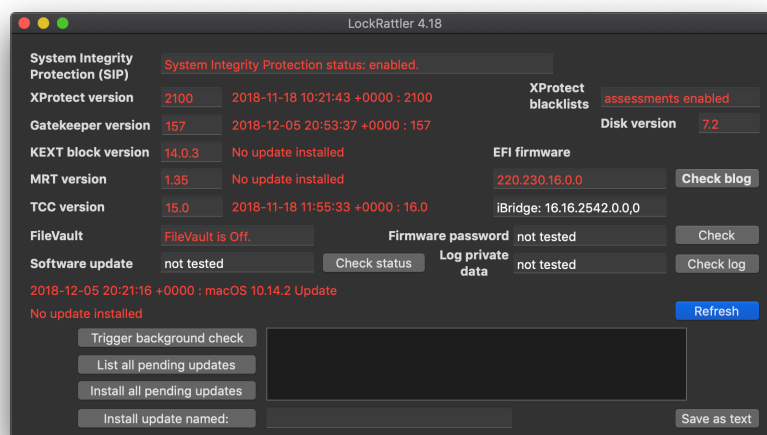
To complete the **Software update** test, click on the **Check status** button and then authenticate as an admin user. To complete the **Log private data** test, click on the **Check log** button and then authenticate as an admin user. To complete the **Firmware password** test, click on the **Check pwd** button and then authenticate as an admin user.



LockRattler has to obtain your authentication in order to check the software update, log, and firmware password statuses. It does not access any of your user files, or change anything on your Mac, and if you'd rather not authenticate, don't click on any of those buttons.

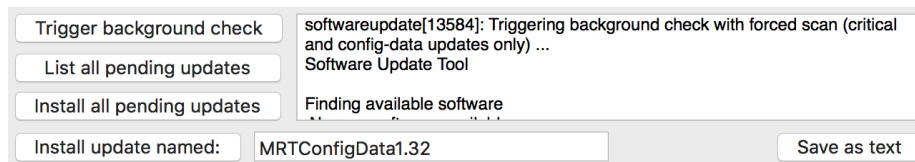
You might already know that some or all of your security data files are up to date, but at this stage it may be helpful to check them against what is supposed to be current. Apple doesn't provide that information, but if you click on the **Check blog** button, a basic browser window will open and connect to one of four special pages on the Eclectic Light Company blog. These display the current versions of XProtect, Gatekeeper, KEXT block, MRT and TCC data files, and the latest applicable security update for the version of macOS which your Mac is running. You can then compare those against the versions listed in the LockRattler window.

After you have run LockRattler for the first time on any given Mac, it stores all the results apart from those obtained after authentication in its preference file. When you run the app again, or click on its **Refresh** button, LockRattler compares the latest results with the previous ones. Those which have changed are displayed using red text, to make it easier to notice any changes. The results which can be shown in red are made clear in the screenshot below.



To check whether your Mac has the latest firmware installed, use the **EFI firmware versions** command in the **Help** menu. This will open the article on the Eclectic Light Company blog which lists current firmware versions for different models. Once again, Apple doesn't provide an official listing, but I maintain that article as well as I can.

Checking for updates



Each of the four buttons to check for updates does something significantly different:


- **Trigger background check** tells macOS to check in the background for security and other urgent software updates only (not available for El Capitan).
- **List all pending updates** asks Apple's servers what updates of all kinds, including 'silent' security updates, are currently available for your Mac.
- **Install all pending updates** asks Apple's servers to provide your Mac with all pending updates, including 'silent' security updates, and to install them immediately.
- **Install update named:** asks Apple's servers to provide your Mac with only the update package which you have named in the adjacent box, and to install it immediately.


In each case, the results are written into the large scrolling text box to the right of the upper three buttons.

When you click on the **Trigger background check** button, LockRattler runs the following command:

```
sudo softwareupdate --background-critical
```

This first requires you to authenticate as an admin user in order to run. It then instructs your Mac to perform a check for security and other critical software updates in the background. If it finds any such updates available for your Mac, they will be silently downloaded and installed over the next few minutes.

 If you have turned off automatic checks for software updates, this may not work. Because of unreliability, this button is not available when running LockRattler in El Capitan. If you want to run this command in El Capitan, copy and paste the command above into Terminal.

 This action is most suitable if you don't want to install any other updates, only security and other critical software updates, but doesn't force them to be downloaded and installed immediately.


When you click on the **List all pending updates** button, LockRattler runs the following command:

```
softwareupdate -l --include-config-data
```

or, in El Capitan,

```
softwareupdate -l
```

This shouldn't require you to authenticate, even in El Capitan, and asks Apple's servers to provide a list of any and all outstanding software updates, including 'silent' security updates, available for your Mac. It doesn't attempt to download or install any of them, but simply lists all those available in the scrolling text box. This should work even when automatic updates are disabled.

 This action is most suitable when you just want to see which updates are available, but don't want to install them yet. It is also ideal when you just want to install one or two packages: obtain the list of pending updates, select one which you wish to install, copy it, and paste that text into the box next to the **Install update named:** button.


When you click on the **Install all pending updates** button, LockRattler runs the following command:


```
softwareupdate -ia --include-config-data
```

or, in El Capitan,

```
sudo softwareupdate -ia
```

If you are running El Capitan, you will need to authenticate before this command is run, but that is not required in Sierra or later. This tries to connect to Apple's servers, and discover whether there are any outstanding software updates for your Mac. If there are, they will then be automatically downloaded and installed for you. The text box displays the result from that command in full.

 This automatically installs all updates including 'silent' security updates, whether you want them or not. When large updates are available, it may take several hours to complete, during which LockRattler will display a 'busy spinner' to indicate that it is still busy. You may wish to list pending updates first to see what is available first.

 This action is most suitable if you want to have all updates installed immediately, and saves you from having to open the App Store app to download and install them.


When you click on the **Install update named:** button, LockRattler runs the following command:


```
softwareupdate -i --include-config-data updatepackage
```


or, in El Capitan,

```
sudo softwareupdate -i updatepackage
```

where `updatepackage` is the valid name of an available update package. If you are running El Capitan, you will need to authenticate before this command is run, but that is not required in Sierra or High Sierra. This tries to connect to Apple's servers, and download and install the named package for you. The text box displays the result from that command in full.

 This automatically installs only the named package. If that is very large, it may take several hours to complete, during which LockRattler will display a 'busy spinner' pointer to indicate that it is still busy.


 This action is most suitable if you don't want to install all the updates which are available. It's best to list those available using the **List all pending updates** button first, to select and copy the package name from that listing, and to past it into the text box before clicking the button. If the text box is empty, clicking on this button does nothing.

 By default, LockRattler automatically installs all the updates it downloads. If you want to download updates but not install them immediately, you can now change that, as detailed next.

Download but don't install updates automatically

By default, LockRattler both downloads and installs updates. There are occasions when you may prefer only to download updates for the time being, and decide whether to install them later. For example, a bug in MRT version 1.68 caused problems on many Macs. If you wish to be cautious, you could just download future updates to MRT then, after a couple of days, if the latest update appears to be problem-free, you could install it.

To disable automatic installation, select the **Install Updates** command in the **LockRattler** menu. It will then become unticked and show the words **Download Updates**. Select that again to turn automatic installation back on.

To remind you that updates are only being downloaded, when installation is disabled a  warning triangle is displayed in LockRattler's window, and buttons which normally read **Install** ... are changed to read **Download** ... instead.

Downloaded updates are saved in the /Library/Updates folder, which is automatically opened for you when downloading is complete. Apple's documentation (from 2012) warns that those Installer packages "are not designed to be installed by double-clicking the packages in that directory: always use [softwareupdate] --install or the App Store to actually perform the install." However, in Mojave and later that doesn't appear necessary. Downloading can also result in spurious errors being reported when the update is in fact perfectly good.

Saving the results

Click on the **Save as text** button to save the results out to a text file. There is an example provided at the end of this manual. Note that the time given at the end of that file, and used in the default name of that file too, is that at which the last set of data were obtained by LockRattler, i.e. when the window opened or was last refreshed, whichever is the later.

When you're finished, closing LockRattler's single window will also quit the app.

Interpreting the results

LockRattler runs a total of fourteen tests, each of which is reported in a separate section in its window. You can run them as often as you like, and if you leave the window open, clicking on the **Check** button will run all the tests again.

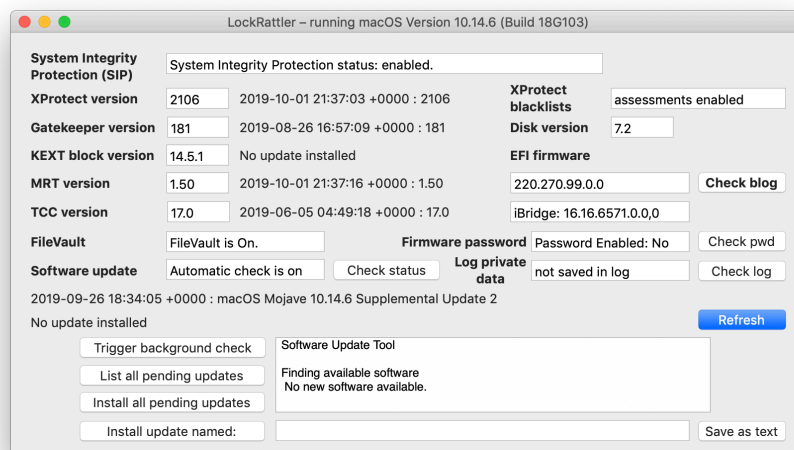
LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur Manual

Howard Oakley <https://eclecticlight.co>

⚠ When run on El Capitan systems, the Gatekeeper Disk version doesn't appear. As this protection didn't appear until Sierra, it does not apply to El Capitan and is therefore omitted from the window and LockRattler's reports. Also omitted is the log privacy test, as that only apply to the unified log which was introduced with macOS Sierra. El Capitan doesn't have any special privacy settings for its more traditional log system.

⚠ When run on El Capitan, Sierra, or High Sierra systems, the TCC version doesn't appear, as this is only (very) important in Mojave and Catalina.

⚠ When run on Catalina or Big Sur systems, the Gatekeeper Disk version is renamed GKE to reflect its changed role.



To check SIP, it runs the shell command

```
csrutil status
```

This should *always* return a statement that SIP is enabled, as shown above. If SIP is disabled, you will need to enable it; details are provided in my blog, or you can call Apple Support. In fact, if it is a new Mac, you should call Apple Support so that they know that Macs are shipping without SIP.

To check XProtect blacklist protection, it runs the shell command

```
spctl --status
```

This should *always* return that assessments are enabled. If they are not, contact Apple Support soonest.

To check whether FileVault (disk encryption) is turned on, it runs the shell command

```
fdesetup status
```

This is an *option* which you control in the **Security & Privacy** pane of System Preferences.

To check firmware, it run the two shell commands

```
system_profiler SPHardwareDataType  
/usr/libexec/firmwarecheckers/eficheck/eficheck --integrity-check
```

The first of these works on all Macs, and returns the same version which is shown in System Information. The second is only run on High Sierra and later and isn't available on Macs

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur Manual

Howard Oakley <https://eclecticlight.co>

equipped with the T2 chip or Apple Silicon Macs; it uses the recent tool `eficheck`, which may return a version number in quite a different format. For Macs without a T2 chip, the upper result box shows the ‘new’ version number, and the lower that given by `eficheck` where available. On Macs with a T2 chip, the upper result box shows the ‘new’ version number for the firmware, and the lower gives the iBridge version number when available. Any errors are reported in the scrolling textbox below.

Firmware is now only updated as part of an Apple macOS upgrade or update, and performed within that installer. Apple doesn’t provide separate copies of firmware which you can install yourself outside of a system update.

To check whether Software Update is set to Automatic, it runs the shell command
`sudo softwareupdate --schedule`
with root privileges, which is why you are prompted to enter your admin password. This is an *option* which you control in the App Store pane of System Preferences, where the box labelled **Install system data files and security updates** (and **Automatically check for updates**) should be ticked (enabled).

To check whether privacy settings are in place for the unified log (Sierra and later), it runs the shell command
`sudo log config --status`
with root privileges, which is why you are prompted to enter your admin password. This is an *option* which is controlled from the command line, and in some tools such as Cirrus.

To check whether the firmware password has been set, it runs the shell command
`sudo firmwarepasswd -check`
with root privileges, which is why you are prompted to enter your admin password. This is an *option* which is normally managed in the **Firmware Password Utility** in Recovery mode, but can also be managed in Terminal’s command line.

The other six checks are of the current versions of the data files used by macOS security protection systems. Apple pushes out silent updates to these, but if you have recently applied a Combo update or your Mac has been away from an Internet connection for some time, your data files may not be up to date.

The files in question are:

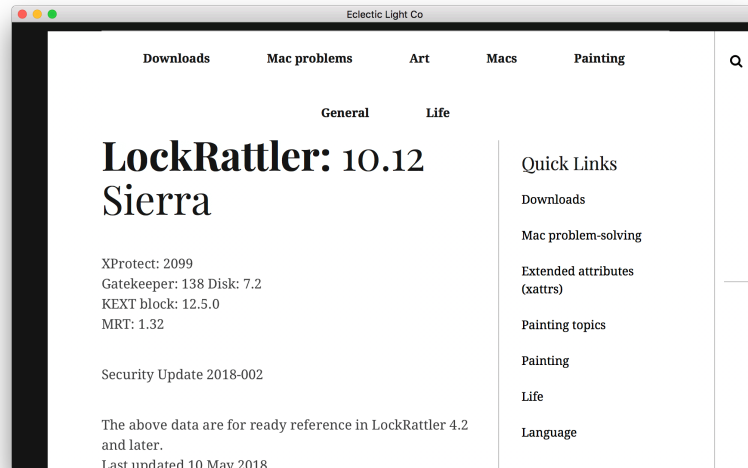
- for XProtect version, `/System/Library/CoreServices/XProtect.bundle` or, for 10.15, `/Library/Apple/System/Library/CoreServices/XProtect.bundle`
- for Gatekeeper version, `/private/var/db/gkopaque.bundle`
- for Gatekeeper disk/GKE version, `/private/var/db/gke.bundle` (Sierra and later only)
- for KEXT block version, `/System/Library/Extensions/AppleKextExcludeList.kext` or, for 10.15, `/Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext`.

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur

Manual

Howard Oakley <https://eclecticlight.co>

- for MRT version, /System/Library/CoreServices/MRT.app or, for 10.15, /Library/Apple/System/Library/CoreServices/MRT.app
- for TCC version, /System/Library/Sandbox/TCC_Compatibility.bundle or, for 10.15, /Library/Apple/Library/Bundles/TCC_Compatibility.bundle.



When you click on the **Check blog** button at the far right of the window, LockRattler opens a browser window, and displays one of three special pages on the Eclectic Light Company blog which list the current versions of those security data files. It determines which version of macOS your Mac is running in order to fetch the correct page for that Mac. You can then check the version numbers listed there against those found.

⚠ Apple doesn't maintain a list of current version numbers. I maintain the lists used by LockRattler myself, and there will be a short delay in updating them when Apple releases each new security update.

I also maintain fuller lists of the current versions of those, related files and EFI firmware versions on my blog at <https://eclecticlight.co> which provide additional information. Direct links are embedded in LockRattler's Help book, which is accessed through the **Help** menu. Also in that menu is the command **Browse updates**, which opens a list of software updates available from the Eclectic Light Company blog.

To view the Eclectic Light Company listing of current firmware version numbers, use the **EFI firmware versions** command in the **Help** menu, which will open the correct article in my blog.

In addition to those basic tests, LockRattler obtains seven useful pieces of information about the updates which have been installed. These are obtained from the record of software installations and updates in /Library/Receipts/InstallHistory.plist.

- Next to the XProtect version, it gives the date and time of the last XProtect update, and the version number for that. That should match the actual version number given.

- Next to the Gatekeeper version, it gives similar information for Gatekeeper's data files, which should match the actual version number given.
- Next to the KEXT block version, it gives similar information for that extension. This may not match the version number given to the left, as on at least two occasions, Apple has updated this as part of a security or system software update.
- Next to the MRT version, it gives similar information for MRT, which should match the actual version number given.
- Next to the TCC version, it gives similar information for TCC, which should match the actual version number given.
- Below **Software update**, it gives the date and time of the last OS X / macOS update installed, and its official name.
- Below that, it gives the date and time of the last Security Update installed, and its official name. If there has been no Security Update installed since the last macOS update, LockRattler now reports that as **No security update installed**.

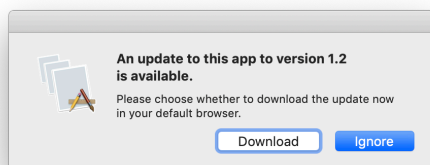
⚠ Dates and times given for software updates are stated in UTC, not local time, for consistency no matter where you are. Similarly, results given for tests are exactly those supplied by macOS, and are not interpreted or altered in any way.

Checking for updates

Whenever you open LockRattler, it may check to see if an update to the app is available. This doesn't use the popular Sparkle mechanism for updating in place, but works as detailed here.

Once the app has successfully completed its integrity check, it looks at whether update checking has been turned off in its preferences file. If that has, it abandons any attempt to check for updates. If checking is allowed, it then checks when it last checked for updates. If that was more than 12 hours ago, it continues to perform the check. It then connects to my GitHub server, from where it downloads a list of current versions of my apps. It doesn't upload any data to the GitHub server at all, and no statistics beyond GitHub normal connection figures are collected either: no personal identifiers are recorded.

If there is an update available, LockRattler then checks that its location is on this WordPress blog, and posts a dialog which invites you to download the update.



If you click on the **Download** button, it then points your default browser at that update, which should trigger the update to be downloaded to your normal downloads folder. The update is received as a regular Zip archive, and is exactly the same as you would download

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur Manual

Howard Oakley <https://eclecticlight.co>

from the Downloads page on my blog. It also carries a quarantine flag, so that when you unZip it and install the app inside, it undergoes normal first run ‘Gatekeeper’ security checks. If you click on the **Ignore** button, LockRattler won’t remind you about it again for another 12 hours.

An additional item at the end of the Help menu explains the update status. If no update check is performed, or the check fails, the last item reads **Update not checked**. If the check is performed and update information is obtained, even when no update is available or you decline to download it, that menu item reads **Checked for update** and is ticked (but still disabled).

You can customise this behaviour by changing LockRattler’s preferences. The keys to use are:

- `noUpdateCheck`, a Boolean. When set to `true`, this disables all update checking. Default is `false`.
- `updateCheckInt`, a real number (Double). When set to a value greater than 1.0, the minimum time interval between checks, in seconds. Default is 43200, which is 12 hours. If you set it to any value less than 1, LockRattler will reset it automatically to that default.

To change either of these, use a Terminal command of the form

```
defaults write co.eclecticlight.LockRattler updateCheckInt '10'
```

which works properly through the preferences server `cfprefsd`.

Support

Additional information and support are available from the **LockRattler Support** command in the Help menu. This opens the app’s product page in your default browser, providing useful information about updates and a link to the support page on which you can post comments and questions.

Example Text File Output (Mojave)

```
System Integrity Protection status: enabled.
XProtect blacklist assessments enabled
XProtect version (/System/Library/CoreServices/XProtect.bundle) 2100
  Last installed update 2018-09-28 06:59:41 +0000 : 2100
Gatekeeper version (/private/var/db/gkopaque.bundle) 156
  Last installed update 2018-10-30 19:51:44 +0000 : 156
Gatekeeper disk/GKE version (/private/var/db/gke.bundle) 7.2
KEXT block version (/System/Library/Extensions/AppleKextExcludeList.kext) 14.0.3
  Last installed update 2016-11-03 03:33:02 +0000 : 12.1.2
MRT version (/System/Library/CoreServices/MRT.app) 1.35
  Last installed update 2018-06-19 21:18:29 +0000 : 1.35
TCC version (/System/Library/Sandbox/TCC_Compatibility.bundle) 14.0
  Last installed update No update installed
  Last installed macOS update 2018-10-30 19:33:35 +0000 : macOS 10.14.1 Update
  Last installed security update 2018-07-09 21:17:12 +0000 : Security Update 2018-004
10.12.6
EFI firmware version installed 161.0.0.0.0
EFI firmware version by efichk IM171.88Z.F000.B00.1809251200
Software update checks:
Software Update Tool
```

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur

Manual

Howard Oakley <https://eclecticlight.co>

```
Finding available software
No new software available.
```

```
Log file private data: not saved in log
FileVault is Off.
Firmware password: Password Enabled: No
Software update: Automatic check is on.
Checked by LockRattler 4.25 at: 2019-10-13 10:41:36 +0000
```

Change List

4.28 release:

- added reporting of Apple Silicon firmware version (iBoot) and changed title.

4.27 release:

- added option for downloads only.

4.26 release:

- final tweaks for Big Sur
- Universal App.

4.25 release:

- fixed (at last, I hope) problems with updating bundle versions after installing updates.
- added support for Big Sur.

4.24 release:

- added support for KEXT exclusion extension for Catalina.

4.23 release:

- changed handling of GKE bundle info for Catalina
- updated Help book for GKE, Catalina and more
- added size and position saving for windows
- adjusted main window controls and outputs
- various minor improvements, particularly for Catalina
- ported to Swift 5.1 in Xcode 11.1.

4.22 release:

- added new paths for Catalina beta 4
- added macOS version to saved report
- added new blog versions page for Catalina
- updated Help book.

4.21 release:

- disabled KEXT block for Catalina
- tweaked system updates for Catalina
- added automatic check for updates.

4.20 release:

- changed window title to give current macOS version
- added code to perform signature check on each launch.

4.19 release:

- added LockRattler Support command
- ported to Swift 5 and Xcode 10.2.

4.18 release:

- added checks to see if results have changed, and display in red if they have

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur
Manual

Howard Oakley <https://eclecticlight.co>

- greatly extended preferences file to store previous results
- updated Help book accordingly.

4.17 release:

- offers default report file name incorporating date and time
- timestamp in report changed to the time at which checks were last run.

4.16 release:

- reports TCC updates correctly
- now reports **No security update** installed if none has been installed since last macOS update
- removed terminating) from iBridge firmware version.

4.15 release:

- detects T2-equipped systems correctly (at last).

4.14 release:

- detects systems which lack efichk tool
- those with T2 chips should not try running efichk, but give iBridge firmware version instead
- added EFI firmware versions link to Help menu.

4.13 release:

- added two EFI firmware checks
- tweaked macOS update detection to find 10.14.1 update properly
- ported to Swift 4.2.1 and Xcode 10.1.

4.12 release:

- added TCC version for Mojave
- revised Help book and docs.

4.11 release:

- built with Xcode 10.0 release and notarized
- fixed (I hope) updating of bundle versions when refreshed
- minor cosmetics in the window.

4.10 release:

- built with Xcode 10B6 and notarized
- added firmware password check
- added Privacy settings window to Help
- minor improvements in window layout, and text file output
- added Mojave page for checking with blog.

4.9 release:

- built with Xcode 10B5
- notarized for macOS Mojave; as the code is unchanged from 4.8, still displays that version number in its window title, etc., although Get Info and its About box show 4.9.

4.8 release:

- replaced IB WebView with WKWebView in view of deprecation of the former
- tidied Tooltips.

4.7.1 release:

- fixed a signing issue with 4.7.

4.7 release:

- added feature to check log privacy setting (Sierra and later)

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur
Manual

Howard Oakley <https://eclecticlight.co>

- reorganised window
- added Mojave as a ‘supported’ system for macOS updates.

4.6 release:

- fixed a typo in the Help book and this document (thanks to Scott for noticing this)
- ported to Swift 4.2 and built using Xcode 10β3.

4.5 release:

- fixed command for installing named updates; this now works
- updated Help book to reflect recent changes
- fixed support for Dark Mode.

4.4 release:

- built in Xcode 10.0 beta, under Mojave
- added **Browse updates** command
- added support for Dark Mode in Mojave.

4.3 release:

- added **Refresh** button
- made main window fixed size, as growing window was purposeless
- updated Help book to clarify updates with respect to ‘silent’ security updates.

4.2 release:

- added **Check blog** button and browser.

4.2b1:

- Put command execution into background thread
- Added busy spinner
- Added **Install update named:** button and text box
- Updated Help book.

4.1 release:

- Removed Trigger background check when running on El Capitan due to errors
- New app icon, thanks to blackspike.com
- Updated Help book and copyright info.

4.1b4:

- Added Trigger background check
- Added List all pending updates
- Updated Help book
- Completed Tooltips.

4.1b3:

- Changed Check for security updates command for El Capitan only
- Detects which version of macOS is running, and decides on window contents accordingly
- More meaningful text generated when no updates are found
- Removed Gatekeeper Disk info from El Capitan reports.

4.1b2:

- Set bundle version checks to return suitable message if bundle not found
- Set El Capitan Check for security updates to use elevated privileges.

4.1b1:

- Added Check for security updates feature
- Included access to update history, giving results in additional text fields.

LockRattler 4.28 for macOS El Capitan, Sierra, High Sierra, Mojave, Catalina and Big Sur

Manual

Howard Oakley <https://eclecticlight.co>

4.0 release:

- Titled window *LockRattler* rather than default *Window*.

4.0b2:

- Altered behaviour to quit when the window is closed
- Rebuilt to standard, rather than archive, package.

4.0b1:

- Completely rewritten in Swift 4 and built using Xcode 9.2.

9 November 2020.