

## Issues

| #  | Project    | Tracker | Status | Priority | Subject   | Assignee     | Related issues | Security Fix |
|----|------------|---------|--------|----------|---|--------------|----------------|--------------|
| 14 | CipherShed | Bug     | New    | Normal   | Fixes urls in ui (/applink? links)  |              | Related to #25 |              |
| 21 | CipherShed | Bug     | New    | High     | Method of mounting may be exploited   |              |                |              |
| 26 | CipherShed | Bug     | New    | Normal   | Large External Drive Support on Mac (>512byte sector size)  |              |                |              |
| 23 | CipherShed | Bug     | New    | Normal   | Windows 8 / 8.1 Fast Startup  | Rocki H      |                |              |
| 31 | CipherShed | Bug     | New    | Normal   | there is duplicate code for password character checking   | Jason Pyeron | Related to #30 |              |
| 37 | CipherShed | Bug     | New    | High     | Open Crypto Audit Project issues  |              |                |              |
| 38 | CipherShed | Bug     | New    | High     | Weak Volume Header key derivation algorithm   |              | Blocked by #49 |              |
| 39 | CipherShed | Bug     | New    | High     | Sensitive information might be paged out from kernel stacks   |              |                |              |
| 40 | CipherShed | Bug     | New    | High     | Multiple issues in the bootloader decompressor  |              |                |              |
| 41 | CipherShed | Bug     | New    | High     | Windows kernel driver uses memset() to clear sensitive data   |              |                |              |
| 42 | CipherShed | Bug     | New    | High     | TC_IOCTL_GET_SYSTEM_DRIVE_DUMP_CONFIG kernel pointer disclosure                                       |              |                |              |
| 43 | CipherShed | Bug     | New    | High     | IOCTL_DISK_VERIFY integer overflow  |              |                |              |
| 44 | CipherShed | Bug     | New    | High     | TC_IOCTL_OPEN_TEST multiple issues  |              |                |              |
| 45 | CipherShed | Bug     | New    | High     | MainThreadProc() integer overflow   |              |                |              |
| 46 | CipherShed | Bug     | New    | High     | MountVolume() device check bypass   |              |                |              |
| 47 | CipherShed | Bug     | New    | High     | GetWipePassCount() / WipeBuffer() can cause BSOD  |              |                |              |
| 48 | CipherShed | Bug     | New    | High     | EncryptDataUnits() lacks error handling   |              |                |              |
| 56 | CipherShed | Bug     | New    | Low      | FreeBSD support   |              |                |              |
| 59 | CipherShed | Bug     | New    | Low      | optimized rescue disk   |              | Related to #52 |              |
| 63 | CipherShed | Bug     | New    | Normal   | 64 bit gui on 64 bit systems  |              | Related to #65 |              |
| 71 | CipherShed | Bug     | New    | High     | passwords using non-ascii   |              |                |              |
| 72 | CipherShed | Bug     | New    | Normal   | The installation fails, but a message (from windows?) says it succeeds and asks if you want to reboot |              |                |              |
| 73 | CipherShed | Bug     | New    | Normal   | Truecrypt icon showing in taskbar   |              |                |              |
| 74 | CipherShed | Bug     | New    | Normal   | Hardcoded Build date in Help->About window  |              |                |              |
| 76 | CipherShed | Bug     | New    | Normal   | MakeSelfExtractingPackage used in CI cannot have dialog boxes   |              |                |              |
| 78 | CipherShed | Bug     | New    | Normal   | update the ciphershed.org website, automatically  |              |                |              |
| 80 | CipherShed | Bug     | New    | Low      | TEST CASE: ubuntu 14 GUI install  |              |                |              |

| #   | Project    | Tracker | Status      | Priority  | Subject  | Assignee      | Related issues | Security Fix |
|-----|------------|---------|-------------|-----------|--|---------------|----------------|--------------|
| 83  | CipherShed | Bug     | New         | Normal    | deduplicate file names   |               |                |              |
| 84  | CipherShed | Bug     | New         | Normal    | wcsncpy is subject to buffer overflow  |               |                |              |
| 85  | CipherShed | Bug     | New         | Normal    | Dlgcode.c is 9917 lines long, split it up  |               |                |              |
| 88  | CipherShed | Bug     | New         | Normal    | smart card support for containers  |               |                |              |
| 94  | CipherShed | Bug     | New         | High      | CipherShed Volume Creation Wizard: Encryption of Host Protected Area": "Encryption of Host Protected Area" class #32770 not initialized? |               |                |              |
| 95  | CipherShed | Bug     | New         | Normal    | Platform/SystemException.h and Common/Exception.h define the same class/struct   |               |                |              |
| 111 | CipherShed | Bug     | New         | Normal    | ui does not show free drives below c: e.g. A: or B:  | Niklas Lemcke |                |              |
| 116 | CipherShed | Bug     | New         | Normal    | create an option for private/global volume mounting  |               |                |              |
| 108 | CipherShed | Bug     | New         | Urgent    | Open Crypto Audit Project TrueCrypt CS-TC-2 - AES implementation susceptible to cache-timing attacks                                     |               |                |              |
| 118 | CipherShed | Bug     | New         | Normal    | upgrading truecrypt fails if truecrypt is pinned to the taskbar  |               |                |              |
| 107 | CipherShed | Bug     | New         | Immediate | Open Crypto Audit Project TrueCrypt CS-TC-1 - CryptAcquireContext may silently fail in unusual scenarios                                 |               |                |              |
| 109 | CipherShed | Bug     | New         | High      | Open Crypto Audit Project TrueCrypt CS-TC-3 - Keyfile mixing is not cryptographically sound  |               |                |              |
| 22  | CipherShed | Bug     | In Progress | High      | Change name of software for "1.0" release.   | Jason Pyeron  |                |              |
| 110 | CipherShed | Bug     | New         | High      | Open Crypto Audit Project TrueCrypt CS-TC-4 - Unauthenticated ciphertext in volume headers   |               |                |              |
| 123 | CipherShed | Bug     | New         | Normal    | losetup anomaly with OpenSUSE 13.1   |               |                |              |
| 51  | CipherShed | Bug     | In Progress | Normal    | GUID Partition Table (GPT)   | Jason Pyeron  | Related to #55 |              |
| 55  | CipherShed | Bug     | In Progress | Normal    | Unified Extensible Firmware Interface (UEFI)   | Jason Pyeron  | Related to #51 |              |
| 30  | CipherShed | Bug     | Resolved    | Normal    | Allowed character description is wrong   |               | Related to #31 |              |
| 27  | CipherShed | Bug     | Resolved    | High      | Audit of 04af5c7 - Buffer Overflow: sprintf  |               |                |              |
| 28  | CipherShed | Bug     | Resolved    | Normal    | Audit of 04af5c7 - Buffer Overflow: strcat   |               |                |              |
| 29  | CipherShed | Bug     | Resolved    | Normal    | Audit of 04af5c7 - Buffer Overflow: strcpy   | Jason Pyeron  |                |              |
| 49  | CipherShed | Bug     | Resolved    | High      | use a unit testing framework   |               | Blocks #38     |              |
| 77  | CipherShed | Bug     | Resolved    | High      | boot loader is too big, regression on ff4d0578aff9269fdb654a213c850ce576fafd0a   |               |                |              |
| 86  | CipherShed | Bug     | Resolved    | Normal    | Make ciphershed window titlebars different   |               |                |              |
| 101 | CipherShed | Bug     | Resolved    | Normal    | boot loader password prompt takes 100% cpu in VM   |               |                |              |
| 105 | CipherShed | Bug     | Resolved    | Low       | Debian Jessie Complication Error: wx3.0  |               |                |              |
| 112 | CipherShed | Bug     | Resolved    | Normal    | uninstall on windows does not list version info  |               |                |              |
| 113 | CipherShed | Bug     | Resolved    | Normal    | remove the donate screen from the installer  |               |                |              |

| #   | Project    | Tracker | Status   | Priority  | Subject   | Assignee     | Related issues | Security Fix |
|-----|------------|---------|----------|-----------|---|--------------|----------------|--------------|
| 117 | CipherShed | Bug     | Resolved | High      | Failure to function when compiled with GCC 5                                  |              |                |              |
| 119 | CipherShed | Bug     | Resolved | Immediate | DLL side loading attack vulnerability   | Jason Pyeron |                |              |
| 104 | CipherShed | Bug     | Resolved | Low       | wxgtk 2.9, CommandLineInterface, ambiguous overloaded function calls          |              |                |              |
| 125 | CipherShed | Bug     | Resolved | Normal    | Makefile for bootloader fails on case sensitive filesystem                    |              |                |              |
| 126 | CipherShed | Bug     | Resolved | Normal    | VS launcher breaks if using multiple VS and the default is not the one for CS |              |                |              |
| 127 | CipherShed | Bug     | Resolved | Normal    | remove #if 0 code   | Jason Pyeron |                |              |
| 115 | CipherShed | Bug     | Resolved | High      | fails to build on stretch due to overloaded constructors                      |              |                |              |
| 10  | CipherShed | Feature | New      | Low       | Two-factor Pre-boot-authentication with USB stick and Password                |              |                |              |
| 11  | CipherShed | Feature | New      | Low       | Cipher set enablement   |              |                |              |
| 32  | CipherShed | Feature | New      | Normal    | truecrypt.ch ideas thread   |              |                |              |
| 33  | CipherShed | Feature | New      | Normal    | windows comamnd line volume creation  |              |                |              |
| 34  | CipherShed | Feature | New      | Normal    | windows mount point support   |              | Related to #60 |              |
| 36  | CipherShed | Feature | New      | Normal    | support multiple actors to open an encrypted volume                           |              |                |              |
| 50  | CipherShed | Feature | New      | Normal    | Linux FDE   |              | Related to #5  |              |
| 52  | CipherShed | Feature | New      | Low       | recovery utility & tools  |              | Related to #59 |              |
| 53  | CipherShed | Feature | New      | Low       | Portable / non-admin volume browser   |              |                |              |
| 54  | CipherShed | Feature | New      | Low       | Self Destruct Password  |              |                |              |
| 57  | CipherShed | Feature | New      | Normal    | Skein support   |              |                |              |
| 58  | CipherShed | Feature | New      | Low       | Tablet / Touch screen / non-keyboard boot support                             |              |                |              |
| 60  | CipherShed | Feature | New      | Normal    | Enhanced UX - shell extension for container management                        |              | Related to #34 |              |
| 61  | CipherShed | Feature | New      | Normal    | optionally support TPM  |              |                |              |
| 62  | CipherShed | Feature | New      | Normal    | Administrative Configuration for Enterprise IT                                |              |                |              |
| 65  | CipherShed | Feature | New      | Normal    | pure 64 bit version for windows   |              | Related to #63 |              |
| 66  | CipherShed | Feature | New      | Normal    | provide robust API for usermode interaction with kernel driver                |              |                |              |
| 67  | CipherShed | Feature | New      | Normal    | print a backup  |              |                |              |
| 69  | CipherShed | Feature | New      | Low       | integration test: mounting and sharing volumes                                |              |                |              |
| 70  | CipherShed | Feature | New      | Normal    | track git info in build   |              |                |              |
| 75  | CipherShed | Feature | New      | Low       | code coverage - ConvertUTF.c  |              |                |              |
| 79  | CipherShed | Feature | New      | Low       | document a list of file systems compatible with Hidden Volume usage           |              |                |              |

| #   | Project    | Tracker | Status   | Priority | Subject  | Assignee          | Related issues                                | Security Fix |
|-----|------------|---------|----------|----------|--|-------------------|---|--------------|
| 81  | CipherShed | Feature | New      | Normal   | Decrypt System drive via commandline   |                   |   |              |
| 82  | CipherShed | Feature | New      | Normal   | add sparse file detection to non-windows versions  |                   |   |              |
| 87  | CipherShed | Feature | New      | Low      | support multiple hidden volumes  |                   |   |              |
| 89  | CipherShed | Feature | New      | Normal   | Support the Common Criteria Collaborative Protection Profile for Full Disk Encryption      |                   |   |              |
| 90  | CipherShed | Feature | New      | Normal   | cipher setting preference file   |                   |   |              |
| 91  | CipherShed | Feature | New      | Normal   | use linked libraries in kernel driver to isolate logical units and later support plugins   |                   |   |              |
| 92  | CipherShed | Feature | New      | Normal   | allow change of cipher/key on encrypted container without decrypting                       |                   |   |              |
| 93  | CipherShed | Feature | New      | Normal   | support "quick" encrypt for new media (especially flash/SSD)                               |                   |   |              |
| 96  | CipherShed | Feature | New      | Normal   | installer to incorporate a post-installation quick-start wizard                            |                   |   |              |
| 97  | CipherShed | Feature | New      | Normal   | Suggestion 1 — Do not use unknown terminology  | Niklas Lemcke     |   |              |
| 98  | CipherShed | Feature | New      | Normal   | Suggestion 2 — Do not misuse native UI controls  | Niklas Lemcke     |   |              |
| 102 | CipherShed | Feature | New      | Normal   | support for serial console in bootloader   |                   |   |              |
| 99  | CipherShed | Feature | New      | Normal   | Suggestion 3—Separate required and optional input parameters                               |                   |   |              |
| 100 | CipherShed | Feature | New      | Normal   | Suggestion 4—Display the consequences of an action immediately (Immediacy of consequences) |                   |   |              |
| 121 | CipherShed | Feature | New      | Normal   | Support "not" burning CD on encrypting disk operation                                      |                   | Related to #68                                |              |
| 122 | CipherShed | Feature | New      | Normal   | support key escrow   |                   | Related to #68                                |              |
| 124 | CipherShed | Feature | New      | Normal   | investigate switch to FUDforum from phpBB  |                   |   |              |
| 35  | CipherShed | Feature | Resolved | High     | use Doxygen  |                   |   |              |
| 1   | CipherShed | Task    | New      | Normal   | Detailed review of Windows constant strings  | Paweł Zegartowski | Related to #2                                 |              |
| 2   | CipherShed | Task    | New      | Normal   | Upgrade installer to uninstall TrueCrypt   |                   | Related to #1, Related to #13, Related to #16 |              |
| 3   | CipherShed | Task    | New      | Normal   | Finish initial bitmaps and icons   |                   |   |              |
| 4   | CipherShed | Task    | New      | Normal   | Get Windows executable signing key   | Bill Cox          |   |              |
| 5   | CipherShed | Task    | New      | Normal   | Linux build, installer, VM   | Kyle Marek        | Related to #50                                |              |
| 6   | CipherShed | Task    | New      | Normal   | Windows build, installer, VM   | Bill Cox          |   |              |
| 7   | CipherShed | Task    | New      | Normal   | Mac build, installer, VM   | Jason Pyeron      |   |              |
| 8   | CipherShed | Task    | New      | Normal   | Get graphics artist to work on artwork, icons  |                   |   |              |

| #   | Project    | Tracker | Status      | Priority | Subject   | Assignee                    | Related issues | Security Fix |
|-----|------------|---------|-------------|----------|---|-----------------------------|----------------|--------------|
| 9   | CipherShed | Task    | New         | Normal   | Create check-list of features to be tested                    | Pier-Luc Caron<br>St-Pierre |                |              |
| 13  | CipherShed | Task    | New         | Normal   | List of all version numbers                                   | Rocki H                     | Related to #2  |              |
| 15  | CipherShed | Task    | New         | Normal   | Create Gnu Info page  | Eugene Wang                 | Related to #12 |              |
| 16  | CipherShed | Task    | New         | High     | Create list of all installed files / registry keys (Windows). | Rocki H                     | Related to #2  |              |
| 17  | CipherShed | Task    | New         | Normal   | Create debian packaging                                       |                             |                |              |
| 18  | CipherShed | Task    | New         | Normal   | Create rpm packaging  |                             |                |              |
| 19  | CipherShed | Task    | New         | Normal   | Create pkgbuild for arch                                      |                             |                |              |
| 20  | CipherShed | Task    | New         | Normal   | Create dmg for os x   |                             |                |              |
| 24  | CipherShed | Task    | New         | Normal   | Add Windows 8 / Server 2012                                   | Rocki H                     |                |              |
| 25  | CipherShed | Task    | New         | Normal   | Broken applinks   |                             | Related to #14 |              |
| 64  | CipherShed | Task    | New         | Normal   | Rewrite or remove LongReverse in Common/Dlgcode.c             |                             |                |              |
| 103 | CipherShed | Task    | New         | Low      | Const Correctness   |                             |                |              |
| 106 | CipherShed | Task    | New         | Low      | Disable GitHub issue tracker                                  |                             |                |              |
| 114 | CipherShed | Task    | New         | Normal   | Real, unified makefiles                                       | Kyle Marek                  |                |              |
| 12  | CipherShed | Task    | In Progress | Normal   | Write Documentation   | Eugene Wang                 | Related to #15 |              |