HAGIWARA Solutions

Portable Malware Scanner

Linux Version Software Manual

Thank you for purchasing the VaccineUSB3 (hereinafter referred to as "this product"). This manual explains how to use the Linux version software of this product. Please read this manual carefully to use this product correctly.

*For basic information about VaccineUSB3, please refer to the Windows manual.

Content

1 Before Use

The Vaccine USB is a licensed product that contains anti-malware application program with the scan engine of Trellix of the United States (hereinafter called “Trellix”) and updates, including virus definition files (hereinafter called “Trellix Programs”).Before start to use your Vaccine USB, we ask you to read and acknowledge the license conditions (including definition of Vaccine USB, licensing, prohibitions and limitations, disclaimers, and warrantee) bundled with Vaccine USB that provides the terms of use between Hagiwara Solutions Co., Ltd., and you on Trellix Programs contained on Vaccine USB. The start of your using Vaccine USB shall constitute your agreement to the license conditions.

Precaution Instructions for Use

For proper use of Vaccine USB, be sure to read the precaution instructions given below and thoroughly understand the instructions when using Vaccine USB. Be advised beforehand that malfunctions, problems, or loss/damage of data of the devices to which Vaccine USB is connected for use, as well as malfunctions or problems of Vaccine USB caused by improper use are out of the scope of warranty.

Indications of Warning Signs

Caution	This sign indicates possibilities of causing human death or injuries.
Warning	This sign indicates possibilities of causing human injuries or damage to property.

Caution

- When using Vaccine USB while connecting it to a device, follow the warnings and cautions provided by the manufacturer of the device to which Vaccine USB is connected.
- Never use at voltages other than instructed. Ignition, fire, heat generation, or electric shock can result.
- Do not use Vaccine USB while the device for which Vaccine USB is applied for virus scan, deletion, or isolation is in operation. The performance of the device might be affected
- Do not use Vaccine USB with wet hands. Electric shock or malfunctions can result.
- Do not leave Vaccine USB within reach of small children or infants. Swallowing it or its cap poses danger of choking. If swallowed, immediately seek medical consultation
- Do not use while walking or driving. Accidents might result.
- Do not use Vaccine USB where water is used or humidity is high. Electric shock, fire, or malfunctions can result.
- In case liquids or foreign objects enter Vaccine USB or the device to which Vaccine USB is connected, or in case smoke or an unusual smell comes out of Vaccine USB or the connected device, immediately turn off the power supply to the device and plug off the power cable from the outlet. Continued use can result in electric shock or fire.
- Before touching Vaccine USB, remove the static electricity from the body by touching metals, etc. The static electricity can cause damage or erase the data.
- Do not bend forcibly, drop, scratch, or load down with heavy objects. Malfunctions can result.
- In case the connector of Vaccine USB is soiled or dusted, remove with a dry, clean cloth. Use in the soiled state can result in malfunctions.
- Do not remove Vaccine USB from the device or turn the device off while data is written on or read from Vaccine USB. The data can be damaged or deleted, and Vaccine USB can be out of order.

Warning

- When using Vaccine USB while connecting it to a device, follow the warnings and cautions provided by the manufacturer of the device to which Vaccine USB is connected.
- Be sure to back up the data that is saved or to be saved on Vaccine USB. Be advised that Hagiwara Solutions Co., Ltd. bears no responsibility for the loss or damage of the programs or data saved in Vaccine USB.
- The Vaccine USB has a lifespan due to its use of flash memory. (Warranty is valid for the licensed period of Vaccine USB. The maximum warranty period is five years.) After use over a long period of time, data will not be saved or retrieved properly.
- When formatting Vaccine USB, be sure that necessary data is not saved on Vaccine USB.
- We grant you a nonexclusive, nontransferable right to use the Product containing the Trellix programs. The Product is provided solely for your use.or any affiliated company to which you may authorize us or our distributors to perform the audits set forth in the License Agreement. In no event, whether in Japan or abroad. The Product may not be rented or transferred to any third party under any circumstances, whether in Japan or abroad. If you intend to export the Product overseas, you must comply with all applicable export laws, regulations, and procedures, both domestic and international.,If you should export the Product overseas, you must fully comply with all relevant export laws, regulations, and procedures, both domestic and foreign.
- The Vaccine USB is packaged for delivery inside Japan. When exporting overseas, be advised that you package the goods for exporting.
- When you are to execute virus scan on your own, be sure to download the latest virus definition files. The latest virus information shall be confirmed on Trellix's or other related websites.
- The Trellix Programs embedded in Vaccine USB do not remove the detected computer viruses but instead delete or isolate the infected files. (The infected files will not be deleted when it was set to Virus Scan Only mode.) If the OS was infected, the program deletes or isolates the infected OS file, and the host device may be left unusable until it is reinstalled with an uninfected OS.
- Viruses that have infected a system file cannot be deleted or isolated at times. However, dedicated deletion tools available for download at Trellix's Website might be able to delete such viruses.
- Viruses that have infected the system memory cannot be deleted or isolated. Confirm the deletion method on Trellix's Website.
- New viruses are being discovered on a daily basis. Execute virus scans with the latest definition files, otherwise viruses may not be detected, deleted or isolated.
- In case the registry has been overwritten by a virus and such virus has been deleted or isolated, the system may not reboot properly since Vaccine USB does not have a function for restoring the registry.
- Once the licensed period of Vaccine USB has expired, the latest virus definition file will no longer be available for download. After the termination of the license period, Trellix Programs provide no protection and will not be guaranteed. Hagiwara Solutions Co., Ltd., or the retailer bears no responsibility for any damage caused by continued use of Vaccine USB after the license period
- There are viruses that cannot be deleted or isolated by Vaccine USB. For such viruses, check the Trellix database and other information to take necessary actions.
- The Vaccine USB can detect the viruses addressed by Trellix when the pattern files were updated to the latest ones. It does not guarantee the detection of every virus. There are cases where it fails to detect a virus in some files including encrypted files or compressed files with password.

Cautions for Storage

Do not keep the product in the following locations. The Vaccine USB can be deteriorated, or electric shock or fire can result.

- Where exposed to direct sunlight
- Where water might leak and wet
- Around heating equipment or fire
- Under high temperatures (over 50°C) and high humidity (over 85%) where dew condensation can occur or temperature can change drastically
- Where it is not level, or the foundation is unstable, or vibration is generated.
- Where strong magnetic field or static electricity can be generated
- Dusty place

Product Warranty Regulations

For defects found within the warranty period of Vaccine USB, free repair or replacement is available provided such defect is determined to be attributed to Vaccine USB. For damage or malfunctions caused during delivery transport, free repair or replacement is available provided such damage or malfunction is clearly attributed to Hagiwara Solutions Co., Ltd.
The compatibility of Application Programs with your specific purposes cannot be warranted.
Hagiwara Solutions Co., Ltd. shall not be liable for any of the following situations.
Malfunctions or damage due to your mishandling such as drops or impacts during transporting after delivery
Malfunctions or damage due to such natural disasters as earthquakes, lightning, wind, and flood damage or fire for which Hagiwara Solutions Co., Ltd. is not responsible.
Repairs or modification performed by persons other than Hagiwara Solutions Co., Ltd. staff
Hagiwara Solutions Co., Ltd. Malfunctions or damage due to handling that disregards the appriopriate methods of use or precautions described in this Manual
Malfunctions or damage due to the malfunctions or problems of the target device to which Vaccine USB is connected
Loss of or damage to the programs or data recorded on Vaccine USB (Hagiwara Solutions Co., Ltd. shall assume no liability for loss of or damage to the programs or data recorded in the memory, even in case such damage or deletion was caused by a defect in Vaccine USB.)
In case Vaccine USB is lost or stolen and comes into possession of third parties, the recorded data can be leaked. Be sure to secure Vaccine USB since Hagiwara Solutions Co., Ltd. takes no responsibility for indemnifying any loss and damage arising out of such a situation.

Limited Indemnity

In any case, Hagiwara Solutions Co., Ltd. or the retailer accepts no liability for any incidental, indirect, special, or consequential damage, including the loss of profit, use, data, trust or confidence, business interruption, or other similar damage caused in relation to Vaccine USB or liability for lost profit.

2 License Agreement

This document outlines the conditions under which VaccineUSB Software (hereinafter referred to as "the Software") is provided for customer use. Please read this document carefully before installing the Software. This agreement establishes the terms under which the use of the software provided by Hagiwara Solutions Co., Ltd. (hereinafter referred to as "the Company") to the customer (hereinafter referred to as "the Customer") is licensed. The Company grants the Customer the right to use the licensed software in accordance with the following terms. The Customer should read the content of this agreement carefully and may use the licensed software at their own risk only if they agree to the content of this agreement. By using the licensed software, the Customer is deemed to have agreed to each term of this agreement. If the Customer does not agree to each term of this agreement, the Company cannot grant the Customer the right to use the licensed software.

Article 1 (General Provisions)
The licensed software is protected by copyright and other intellectual property laws and treaties, both domestically and internationally. The licensed software is licensed to the Customer by the Company under the terms of this agreement, and the intellectual property rights of the licensed software, including copyrights, belong to the Company and are not transferred to the Customer.

Article 2 (License)
1. The Company grants the Customer a non-exclusive right to use the licensed software.
2. The right to use the licensed software arising from this agreement refers to the right to use the licensed software on electronic devices that support the licensed software, for the Customer's devices, etc.
3. The Customer may not modify, add to, or otherwise alter any part of the licensed software.

Article 3 (Restrictions on Rights)
1. The Customer shall not re-license, transfer, lend, lease, or in any other way allow a third party to use the licensed software.
2. The Customer shall not use the licensed software to infringe on the copyright or other rights of the Company or any third party.
3. The Customer shall not engage in reverse engineering, disassembling, decompiling, or any other source code analysis work in relation to the licensed software.
4. Based on this agreement, the Customer may transfer all rights related to the licensed software, as an integral part of the electronic device on which it is installed, to a transferee, provided that the transferee agrees to the terms of this agreement. However, in such cases, the Customer may not retain any copies of the licensed software and must transfer all aspects of the licensed software (including all components, media, electronic documents, and this agreement).

Article 4 (Rights to the Licensed Software)
All rights related to the licensed software, including copyrights, belong to the Company or the original rights holder (hereinafter referred to as the "Original Rights Holder") who has granted the Company the right to license the use of the software to the Customer under this agreement. The Customer shall not have any rights to the licensed software other than the rights to use granted under this agreement.

Article 5 (Scope of Liability)

1. The Company and the Original Rights Holder do not guarantee that the update data defined in Article 6, Section 2 can be installed correctly, nor do they guarantee that the installation of such update data will not cause damage to the Customer.
2. The Company and the Original Rights Holder do not guarantee that the licensed software is free from errors, bugs, or other defects, that it will operate without interruption, or that its use will not cause damage to the Customer or third parties. They also do not guarantee that the licensed software does not infringe on the intellectual property rights of third parties or that manuals and other documents are error-free.
3. Products, software, or network services other than the licensed software on which the operation of the licensed software depends (including those provided by third parties, the Company, or the Original Rights Holder) may be discontinued or interrupted at the discretion of the provider of such software or network services. The Company and the Original Rights Holder do not guarantee that these products, software, or network services will operate without interruption and normally in the future.
4. The liability of the Company and the Original Rights Holder for damage to the Customer is limited to direct and actual ordinary damages that have occurred to the Customer, except in cases of intentional or gross negligence by the Company or the Original Rights Holder, and is limited to the purchase price of the licensed software that the Customer can prove.
5. The Company and the Original Rights Holder shall not be liable for any lost profits, consequential damages, indirect damages, or damages related to data loss or corruption, regardless of the cause of the obligation or tort.
6. The Company provides technical support related to the licensed software licensed to the Customer only through the Company's designated inquiry contact point. However, the Company may change the reception hours of the contact point and the availability of support at any time without the consent of the Customer. Furthermore, unless a separate contract is concluded between the Customer and the Company, the Company is under no obligation to provide or continue to provide such support.

Article 6 (Copyright Protection and Automatic Updates)

1. The Customer agrees to comply with all relevant domestic and international copyright and other intellectual property laws and treaties when using the licensed software.
2. The Customer must update the licensed software within 90 days following the publication of update data (hereinafter "Update Data") by the Company or a third party designated by the Company on the web for the purpose of improving security features, correcting errors, enhancing update functions, etc. of the licensed software. If more than 90 days pass after the Update Data has been published, the Customer cannot use the old version of the licensed software for any purpose other than updating it. The Customer agrees that (i) the functionality of the licensed software may be added, changed, or removed as a result of such updates, and (ii) the updated licensed software will also be subject to this agreement.

Article 7 (Termination of Agreement)

1. The Company may immediately terminate this agreement if the Customer violates any terms set forth in this agreement.
2. Upon termination of this agreement pursuant to the provisions of the preceding paragraph, the Customer must dispose of or return all of the licensed software to the Company within two weeks from the date of termination. If the Customer disposes of the licensed software, they must immediately submit documentation proving such disposal to the Company.

3. The provisions of Articles 4 and 5, Sections 2 and 3 of Article 7, and Sections 1, 3, 4, and 5 of Article 8 shall remain in effect even if this agreement is terminated pursuant to Section 1 of this Article.

Article 8 (Consent to Use of Data)

The Customer agrees that the Company may collect and use technical information related to the usage of this product (excluding information about the Customer's devices), which is not limited to these, for the purposes of software updates related to the Company's products, product support, and other services to be smoothly provided to the Customer. This information will be collected on a regular basis. The Company may use this information in a manner that does not personally identify the Customer, for the purpose of improving products or providing services or technology to the Customer.

Article 9 (Miscellaneous)

1. This agreement shall be governed by the laws of Japan.
2. If the Customer takes the licensed software outside of the country, they must comply with the applicable ordinances, laws, export control regulations, and orders.
3. Any disputes related to this agreement shall be subject to the exclusive jurisdiction of the district court or summary court located at the Company's head office location in the first instance.
4. If any provision of this agreement is rendered invalid by law, such provision shall remain effective to the extent that it is deemed valid by law.
5. If there are any matters not stipulated in this agreement or any doubts arise regarding the interpretation of this agreement, the Customer and the Company shall discuss and resolve the matter in good faith.

3 Features of Linux Version Software

Malware Scan

Scans files stored on target devices and displays results via screen and LED indicators:

-During malware scan: Red ● LED and blue ● LED flash alternately

-When malware detected: Red ● LED lights up

-When no malware detected: Blue ● LED lights up

Scan Mode Selection

Two scanning modes available:

-Scan Only: Performs malware detection without removal

-Scan + Auto Delete: Performs malware detection and immediate removal upon detection

-Scan + Auto Quarantine: Performs malware detection and immediate quarantine upon detection

Comprehensive Log Management

Automatically records scan results, detected malware details, and system information in detailed log files.

Product Virus Infection Prevention

The product is configured to prevent any file writing. Includes functionality to prevent virus infection, including unknown viruses, when connected to an infected PC.

Configurable Scanning Paths

Enables users to define specific directories or drives for targeted scanning.

Shared License Period and Definition Files with Windows Version

License information activated on Windows PC and downloaded definition files are shared with Linux version software.

Command Line Interface

Linux version software operates via command line interface.

Notes:

- Perform log checking, activation, definition file updates, and license renewal on Windows PC
- License period (activation) and definition files downloaded on Windows PC are shared on Linux
- Windows version software settings do not apply to Linux version
- Linux version includes selected features from Windows version
- "Malware" refers to all harmful software including viruses, worms, trojans, spyware, and any malicious software affecting computers and networks.

4 System Requirements

Interface	USB 2.0 (High Speed/Full Speed) / USB3.0 (Super Speed)
Operating Environment *1*2	CPU: Meets OS minimum requirements -Supports both 64-bit (x64) and 32-bit (x86) Intel architectures. -ARM not supported Memory (physical available): 1GB or more *2GB or more recommended HDD/SSD free space: 1.5GB or more Display resolution: VGA (640x480) or higher
Supported Operating Systems	-Red Hat Enterprise Linux 9(64-bit) -Red Hat Enterprise Linux 8(64-bit) -Red Hat Enterprise Linux 7(64-bit) -Red Hat Enterprise Linux 6(32-bit/64-bit) -CentOS 8(64-bit) -CentOS 7(64-bit) -CentOS 6(32-bit/64-bit) -CentOS 5(32-bit/64-bit) -AlmaLinux OS 9(64-bit) -AlmaLinux OS 8(64-bit) -MIRACLE LINUX 9(64-bit) -MIRACLE LINUX 8(64-bit) -Rocky Linux 9(64-bit) -Rocky Linux 8(64-bit) -Debian12(32-bit/64-bit) -Debian11(32-bit/64-bit) -Debian10(32-bit/64-bit) -Ubuntu Linux 19 ~ 24(64-bit) -Ubuntu Linux 14 ~ 18(32-bit/64-bit) Notes: -Supported OS may change based on Trellix malware scan engine. Our product's OS support may change with future updates.
Required Account/Permissions	-Root user -sudo privileges

*1 USB Mass Storage Class driver and CD-ROM driver must be pre-installed.
*2 Virus definition file size increases daily to handle new viruses. Required memory capacity may increase accordingly.

5 Limitations

✓Multiple Terminal/Session Execution

This software cannot be launched simultaneously from multiple terminals or sessions. Always execute from a single terminal/session.

✓Multiple VaccineUSB3 Connections

Do not connect multiple VaccineUSB3 devices to one terminal. May cause device failure.

✓Encryption and Password Protection

The VaccineUSB3 is unable to scan files secured with encryption or password protection.

✓Operation with Security Software(cgroup,SELinux etc)

Software may not function properly on PCs with security software(cgroup,SELinux, etc) installed. Security software may restrict our software's operations or device access. If falsely detected by security software, please exclude VaccineUSB3 software.

✓Operation with OS/Software Access Restrictions

VaccineUSB3 may be restricted when OS or software limits device access (e.g., device control). In such cases, please exclude VaccineUSB3.

✓Terminal Window Size

Set terminal window size larger than software's single-line display requirements. (Default size usually sufficient) Display may be corrupted if made smaller.

✓Logoff/Suspend During Scanning

VaccineUSB3 may malfunction if Linux OS enters logoff or suspend while scanning. Do not logoff or suspend while VaccineUSB3 is operating.

✓Old Definition File Usage

Linux version cannot use old definition files. Must update definition files after October 2024 (definition file version: 11200 or later). Scan/deletion will not work on Linux with definition file versions before 11200.

✓*About Using in Virtual Environment*

While this product has been tested in certain virtual environments (undisclosed), we do not guarantee operation in all virtual environments. When using in a virtual environment, please verify operation in your specific environment before use.

In some virtualization software, the VaccineUSB3 may not be recognized properly.
Additionally, USB device recognition and mounting processes in virtual environments are not supported.
For any questions or issues related to virtual environments, please contact your virtualization software provider directly.
We do not provide support for these matters.

[Troubleshooting Recognition Issues]
The following methods may improve device recognition:

- Change the USB settings in your virtualization software to USB 2.0 mode
- Try one of these alternative connection methods:
  Direct connection to a USB 2.0 port

Connection via a USB 2.0 compatible hub
Connection using a USB 2.0 cable

✓Regarding Logout and Suspend During Operation

Vaccine USB3 does not support logout or suspend functions of the Linux OS during operation. Please ensure you remain logged in at all times.

6 Usage Flow/Demo Video

Activation & Definition File Update

1:License Start (Activation)	Update definition files on internet-connected Windows PC. Activation occurs and license starts with first definition file update.
2:Definition File Update	Update definition files on an internet-connected Windows PC. Linux version cannot use old definition files. Must update after October 2024 (definition file version: 11200 or later).

Product Usage

3:Malware Scan Execution	Connect to target Linux device and perform malware scan.
4:Check Malware Scan Results (Logs)	When scan completes, malware detection results display on screen. Results are also shown by two LEDs (blue/red) on device. *Check logs saved in Linux on Windows PC.
5:(If Malware Found) Execute Malware Removal	If malware found, check logs on Windows PC to verify virus files safe to remove. After confirmation, perform "Scan + Auto Delete" or "Scan + Auto Quarantine".

Demo Videos about VaccineUSB3 Linux version software are available.
Check Hagiwara Solutions youtube Ch .

7 About the Software

Software Overview

Execution shell name	startuplnx.sh
Execution shell storage location	VaccineUSB3 removable drive (Volume Label:VUSB_LNX)

This software is command-line based. The command overview is as follows:

Command Name	Description
Malware Scan	Scans files on device and detects malware (including viruses). Detects but does not remove viruses.
Malware Scan + Auto Delete	Scans files on device and removes malware (including viruses) upon detection. *Note: Please be careful as it will delete even important files for the PC if they are malware
Malware Scan + Auto Quarantine	Scans files on device and quarantines malware (including viruses) upon detection. *Note: Please be careful as it will quarantine even important files for the PC if they are malware
Help	Displays command information

Command Details

Malware Scan

Item	Content
Command Name	Malware Scan
Function	Scans files on device and detects malware (including viruses). Detects but does not remove viruses.
Command Structure	startuplnx.sh -scan --s <scan targets>
Arguments (Options)	**-scan**:Scans files on device **--s**:Scan Location Option (Note: --s uses two hyphens) Specifies source directory <scan targets> to scan For multiple directories, separate with spaces Without --s, scans all (permitted) files on device **--fast**: This is the high-speed mode. It will be faster on high-spec PCs, etc.
Other	-If you do not specify a scan location, network drives will not be scanned. -To stop scan midway, press Q (usually: shift+q) in terminal. No log remains if stopped.

Malware Scan Command Examples:

To scan all accessible files on device:

sudo sh ./startuplnx.sh -scan

To scan two locations (/home/user/data and /home/user/test)

sudo sh ./startuplnx.sh –scan --s /home/user/data /home/user/test

Malware Scan + Auto Delete

Item	Content
Command Name	Malware Scan + Auto Delete
Function	Scans files on device and detects/removes malware (including viruses).
Command Structure	startuplnx.sh -delete --s <scan targets>
Arguments (Options)	-delete:Scans files and immediately removes detected malware **--s**:Scan Location Option (Note: --s uses two hyphens) Specifies source directory <scan targets> to scan. For multiple directories, separate with spaces. Without --s, scans all (permitted) files on device. **--y**: When performing deletion, a warning message is displayed after executing the command.Warning message: *Are you sure you want to delete the malware? (y/n)* To avoid displaying this warning message, set this option. **--fast**: This is the high-speed mode. It will be faster on high-spec PCs, etc.
Other	-If you do not specify a scan location, network drives will not be scanned. -To stop scan midway, press Q (usually: shift+q) in terminal.No log remains if stopped.

Malware Scan + Auto Delete Command Examples:

To scan and auto-delete from all accessible files:

sudo sh ./startuplnx.sh -delete

To scan and auto-delete from the following two locations:

sudo sh ./startuplnx.sh -delete --s /home/user/data /home/user/test

*Add space between source directories when specifying multiple directories

Malware Scan + Auto Quarantine New!

Item	Content
Command Name	Malware Scan + Auto Quarantine
Function	Scans files on device and detects/quarantines malware (including viruses).
Command Structure	**startuplnx.sh -qt --s <scan targets>**
Arguments (Options)	**-qt**:Scans files and immediately quarantines detected malware **--s**:Scan Location Option (Note: --s uses two hyphens) Specifies source directory <scan targets> to scan. For multiple directories, separate with spaces. Without --s, scans all (permitted) files on device. **--y**: When performing deletion, a warning message is displayed after executing the command.Warning message: *Are you sure you want to quarantine the malware? (y/n)* To avoid displaying this warning message, set this option. **--fast**: This is the high-speed mode. It will be faster on high-spec PCs, etc.
Other	-After executing the quarantine command, the following warning message is displayed for final confirmation. Warning message: Are you sure you want to quarantine the malware? (y/n) To proceed with quarantine, input y and press enter. To cancel quarantine, press n. -If you do not specify a scan location, network drives will not be scanned. -To stop scan midway, press Q (usually: shift+q) in terminal.No log remains if stopped.

Malware Scan + Auto quarantine Command Examples:

To scan and auto-quarantine from all accessible files:

sudo sh ./startuplnx.sh -qt

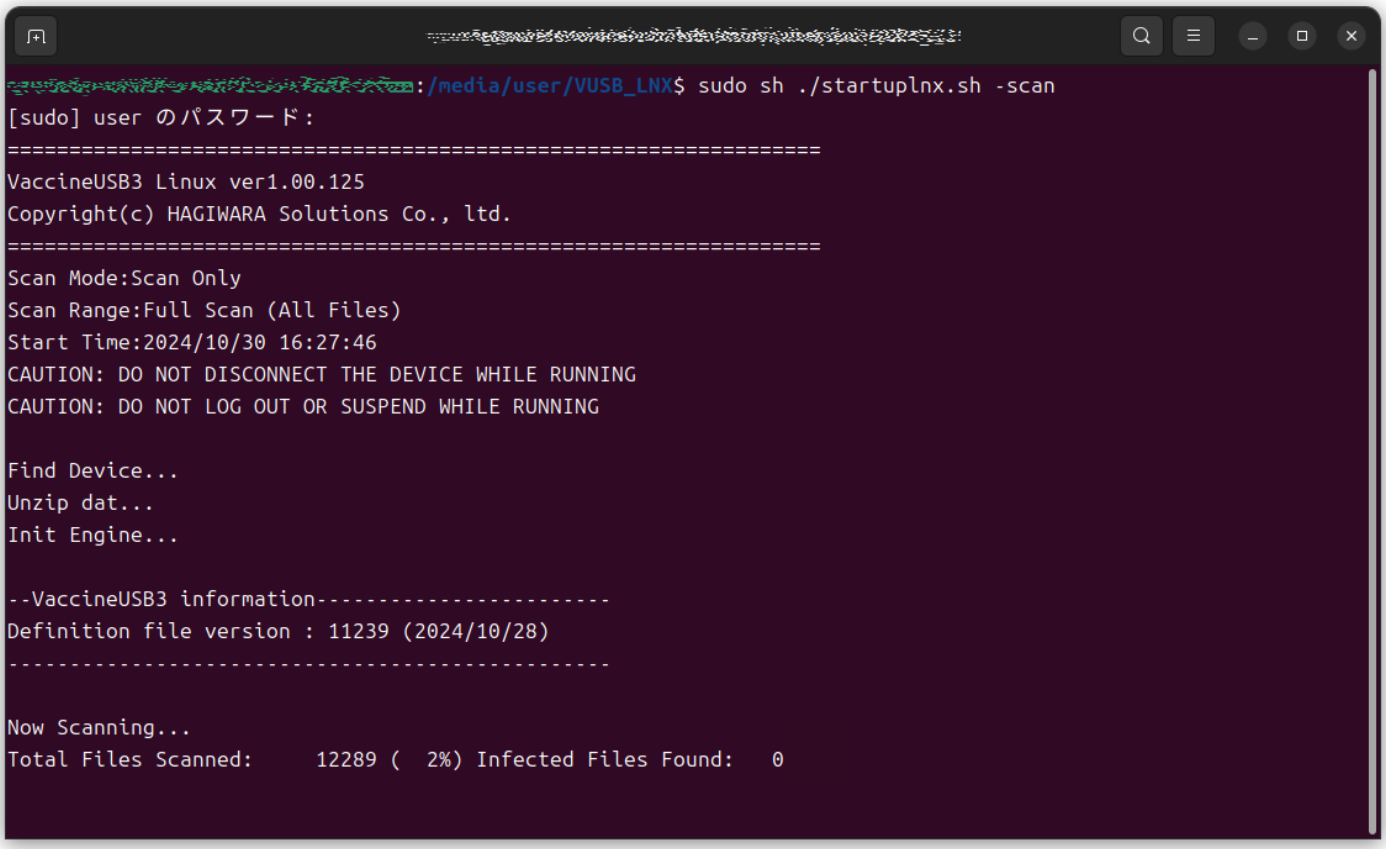
To scan and auto-quarantine from the following two locations:

sudo sh ./startuplnx.sh -qt --s /home/user/data /home/user/test

*Add space between source directories when specifying multiple directories

8 Display Screen & LED Specification

Scanning Display Screen Example:



Screen Component	Description
Version	VaccineUSB3 Linux software version information
Scan Mode	VaccineUSB3 operation mode: - Scan Only: Performs malware scan only - Scan + Auto Delete: Performs scan and immediate deletion. - Scan + Auto Quarantine: Performs scan and immediate quarantine.
Scan Range	VaccineUSB3 scan range: - Full Scan (All Files): Scans all permitted directories - Custom Scan (Selected Files): Scans specified directory(files)
Start Time	Scan start date/time
Definition file version	VaccineUSB3 definition file version
Total Files Scanned	Number of files scanned by VaccineUSB3 (progress %)
Infected Files Found	Number of malware detected by VaccineUSB3.

Post-Scan Display Screen Example:

```
--Scan Summary-----------------------------------
Status:WARNING (Malware was found)
Total Files Scanned:731
Infected Files Found:1
Files Removed:0
Scan End Time:2025/04/10 13:34:19
Total Duration:528 s
-------------------------------------------------
```

Status	Scan results(4 patterns) **-SAFETY (Scan completed successfully. No malware found)** No malware was found **-SAFETY (Scan completed successfully. All detected malware was removed)** Malware was detected but has been removed **-SAFETY (Scan completed successfully. All detected malware was quarantined)** Malware was detected but has been quarantined **-WARNING (Malware was found)** Malware was found **-WARNING (Some malware could not be removed)** Malware was detected but could not be removed **-WARNING (Some malware could not be quarantined)** Malware was detected but could not be quarantined
Total Files Scanned	Total number of files scanned.
Infected File Found	Number of malware detected.
File Removed	Number of malware removed.
Scan End Time	Scan completion date/time.
Total Duration	Scan duration (seconds).

LED Specification

VaccineUSB3 displays scan status/results via built-in LEDs. Results can be checked even on the device without monitors.

Status	Blue LED	Red LED
Idle (Pre-scan)	Off	Off
Scanning	Blinking	Blinking
Scan Summary : No malware was found	On	Off
Scan Summary : Malware was detected but has been removed/quarantined	On	Off
Scan Summary : Malware was found	Off	On
Scan Summary : Malware was detected but could not be removed/quarantined	Off	On
Other Error Occurred	Off	Blinking

9 Usage Instructions

Example usage procedures are explained below. *Steps may vary depending on the environment.

Procedure : Malware Scan

Prerequisites:

USB drive auto/manual mount functionality must be available on Linux system. If the USB drive cannot be mounted, check the Linux manual or guide.

Steps:

1:Connect VaccineUSB3 to the device and auto/manually mount USB drive. *VaccineUSB3 has two drives (CD-ROM and removable drive), but the Linux version uses only removable drive, so CD-ROM mounting is optional.

2:Open mounted USB drive (volume label: VUSB_LNX).

3:Right-click inside folder (not on file or folder icons) and select [Open in Terminal]. The terminal opens. *Elevate to Root privileges if needed.

4:Use following command to scan the device files:

sudo sh ./startuplnx.sh -scan --s <scan targets>

To scan entire the device:
sudo sh ./startuplnx.sh -scan

To scan the following two locations (/home/user/data and /home/user/test):
sudo sh ./startuplnx.sh -scan --s '/home/user/data' '/home/user/test'

Enter privilege elevation password when prompted.

5:The device scan begins. VaccineUSB3's blue/red LEDs flash during scan.
Warning: Disconnecting the VaccineUSB3 during the scanning process may result in the device damage. Please ensure the device remains connected until the scan is complete.

6:The scan results display (screen/LED) after completion. Log saved to VaccineUSB3.

7:Close the terminal and remove VaccineUSB3. Check VaccineUSB3 logs on Windows PC.

Procedure: Malware Scan + Auto Delete

Prerequisites:

USB drive auto/manual mount functionality must be available on Linux system.

If the USB drive cannot be mounted, check the Linux manual or guide.

Steps:

1:Connect VaccineUSB3 to the device and auto/manually mount USB drive.

*VaccineUSB3 has two drives (CD-ROM and removable drive), but the Linux version uses only removable drive, so CD-ROM mounting is optional.

2:Open mounted USB drive (volume label: VUSB_LNX).

3:Right-click inside folder (not on file or folder icons) and select [Open in Terminal].

The terminal opens. *Elevate to Root privileges if needed.

4:Use the following command (example) to scan the device files:

sudo sh ./startuplnx.sh -delete --s <scan targets>

To scan and auto-delete from the entire the device:

sudo sh ./startuplnx.sh -delete

To scan and auto-delete from two locations:

sudo sh ./startuplnx.sh -delete --s '/home/user/data' '/home/user/test'

Enter the privilege elevation password when prompted.

After executing the delete command, the following warning message is displayed for final confirmation.

Warning message: ***Are you sure you want to delete the malware? (y/n)***

To proceed with delete, input '**y**' and press enter. To cancel deletion, press '**n**'.

5. If you press 'y' ,the device scan begins. VaccineUSB3's blue/red LEDs flash during scan.

Warning: Do not disconnect VaccineUSB3 during scan. This may damage the device.

6. The scan results display (screen/LED) after completion. Log saved to VaccineUSB3.

7. Close the terminal and remove VaccineUSB3. Check VaccineUSB3 logs on Windows PC.

Procedure: Malware Scan + Auto Quarantine

Prerequisites:

USB drive auto/manual mount functionality must be available on Linux system.

If the USB drive cannot be mounted, check the Linux manual or guide.

Steps:

1:Connect VaccineUSB3 to the device and auto/manually mount USB drive.

*VaccineUSB3 has two drives (CD-ROM and removable drive), but the Linux version uses only removable drive, so CD-ROM mounting is optional.

2:Open mounted USB drive (volume label: VUSB_LNX).

3:Right-click inside folder (not on file or folder icons) and select [Open in Terminal].

The terminal opens. *Elevate to Root privileges if needed.

4:Use the following command (example) to scan the device files:

sudo sh ./startuplnx.sh -qt --s <scan targets>

To scan and auto-quarantine from the entire the device:

sudo sh ./startuplnx.sh -qt

To scan and auto-quarantine from two locations:

sudo sh ./startuplnx.sh -qt --s '/home/user/data' '/home/user/test'

Enter the privilege elevation password when prompted.

After executing the quarantine command, the following warning message is displayed for final confirmation.

Warning message: ***Are you sure you want to quarantine the malware? (y/n)***

To proceed with quarantine, input '**y**' and press enter. To cancel quarantine, press '**n**'.

5. If you press 'y' ,the device scan begins. VaccineUSB3's blue/red LEDs flash during scan.

Warning: Do not disconnect VaccineUSB3 during scan. This may damage the device.

6. The scan results display (screen/LED) after completion. Log saved to VaccineUSB3.

7. Close the terminal and remove VaccineUSB3. Check VaccineUSB3 logs on Windows PC.

10 About Log

Malware scan (including deletion) results from Linux version software are saved as log files in VaccineUSB3.

Log files are generated for each scan. *View logs on a Windows PC.

Linux Version Software Log Contents

Key	Content
Section [LogFormat] Log Format information	
ver	Log Format version
Section [Scan Result Overview] Scan results overview	
Date	Start date and time of vaccine USB scan
ScanType	Scan type (0: Scan only, 1: Scan + immediate deletion, 3: Scan + immediate quarantine)
ScanResult	Final scan result - No virus: No Virus - Virus found: Virus Found
VirusFiles	Number of viruses detected
Section [PC_Information] PC Information	
CPU Model	CPU Model
ComputerName	Computer Name
Date	Log file creation date/time
IPAddress	IP Address
MacAddress	MAC address
ProductName	Distribution Information
ProductNameS	Distribution Information
ProductVersion	Kernel version
RAM Size	Memory Capacity
UserName	Login username (account name)
GlibVersion	glibc version
Section[DeviceInformation] Device Information	
DeviceID	Number on device case (same as USB serial)
DeviceType	Fixed at 30
DeviceProductName	Fixed at VaccineUSB3
ProductID	Device ProductID
ProductVersion	Product version
USB CD Drive Letter	Mount point of VaccineUSB CD drive
USB Removable Drive Letter	Mount point of VaccineUSB removable disk drive
SerialNumber	Device USB serial number
UniqueID	Reserved for internal purposes.
VendorID	Device VendorID
Section[ScannerVersion] Scan App Information	
AntiVirus	Anti-virus software version

LastUpdate	Virus definition file update date
McAfeeScan	Anti-virus software library version
ScanEngine	Scan engine version
VirusDefinitionFileDate	Virus definition file date/time
VirusDefinitionFiles	Virus definition file version
Section[Scan Setting] App Settings	
Scan Mode	Scan range 0: Full scan 2: Custom scan
Scan Type	Scan type 0: Malware scan 1: Malware scan + auto delete 3: Malware scan + auto quarantine
Section[BootScanSetting] Boot Scan Settings	
BootScanType	Scan type during boot scan (0: Malware scan, 1: Malware scan + auto delete)
Section[TargetList] Scan Target List	
Target#	Scan location path (# is number) *Multiple entries for multiple locations
Section [CustomInformation]Custom information ※Customer can set arbitrarily	
CompanyNameReport	Issuing company name
TargetProductName	Scanned terminal name/product name
VaccineUSBManagementNumber	VaccineUSB management number
Section[License] License Information	
LicenseAlert	Company management number
LicenseLast	License end date
LicenseStart	License start date
LicenseTerm	License duration in days
Section[Result] Scan Result	
StartTime	Scan start date/time
EndTime	Scan end time
TotalTime	Scan duration (seconds)
TotalScanFiles	Total files scanned
VirusFiles	Number of malware detected
DeleteVirusFiles	Number of malware successfully deleted
IsolateVirusFiles	Number of malware successfully quarantined
NoDeleteOrNotIsolateVirusFiles	Number of malware failed to delete/quarantine
ScanResult	Final scan result - No virus: No Virus - Virus found: Virus Found
TotalThread	Number of threads when scanning
Section[Virus***] Detected Malware Information (***:Virus number 001~)	

Path	Malware full path
InfectType	The infect type defined by Trellix.
VirusName	The virus name defined by Trellix.
CleanAction	The malware scan result -CleanActionNoAction : Malware found (no deletion performed) -CleanActionVirusDeleteSuccess : Malware deletion successful -CleanActionVirusQuarantineSuccess : Malware quarantine successful -CleanActionDeleteFail : Malware deletion failed -CleanActionQuarantineFail : Malware quarantine failed
Result	Reserved for internal purposes
Detected Malware Information Example	
Detected Malware Information Example	[Virus001] Path=/home/user/Desktop/eicar.txt InfectType=AVT_TEST VirusName=EICAR test file CleanAction=0x29AA0025:CleanActionVirusDeleteSuccess Result=0x710f0003:KEY_AV_SUMMARY_INFECTED

Key	Content
Section [PC Information in detail] Detailed PC Information (****: (0001~))	
BIOSVersion	BIOS Version
CPUTotal	Number of CPUs
CPUTotalCore	Number of CPU cores
DiskTotal	Number of drives
NetAdapter***	Network card name
NetDate***	IP address lease expiration date
NetGateway***	Default gateway
NetIPAddress***	IP address lease and IPv6 address
NetIPSubnet***	Subnet mask
NetMACAddress***	MAC address
SystemHostName	Host name
SystemManufacturer	Computer manufacturer
SystemModel	Computer model name
SystemProductIdentifyingNumber	Computer serial number
SystemProductUUID	Motherboard UUID
Section [PC Drive] PC Drive Information (:** (01~))	
DriveLetter**	Drive mount point
DriveCapacity**	Drive capacity (GB)
DriveFreeCapacity**	Drive free capacity (GB)
Section [software] Third-party Application Info on PC (****: (0001~))	
Name**	Installed third-party application name
Publisher**	Installed third-party application company name

Version**	Installed third-party application version
Section [Hotfix] Kernel-related Software Info on PC (****: (0001~))	
KBName**	Installed kernel-related software name
KBDate**	Date/time installed kernel-related software was installed

11 Managing Quarantined Files New!

When "Scan + Quarantine" is executed and malware is detected, the malware is quarantined by compressing it into a password-protected ZIP file in a specific folder on the PC.

Quarantined File Overview

The specifications for quarantined files are as follows:

Item	Content
Quarantine Location	Quarantined in the following location on the PC. /var/log/VaccineUSB/isolation
Quarantine File Type	Quarantined files are saved in two formats: 1: ******.tar.zip 2: ******.zip
Quarantine Filename Rule	Quarantine Date/Time_Milliseconds + Extension Ex: 20250303101010_12345678.zip
File Compression Format	Password-protected ZIP compression Password: infected

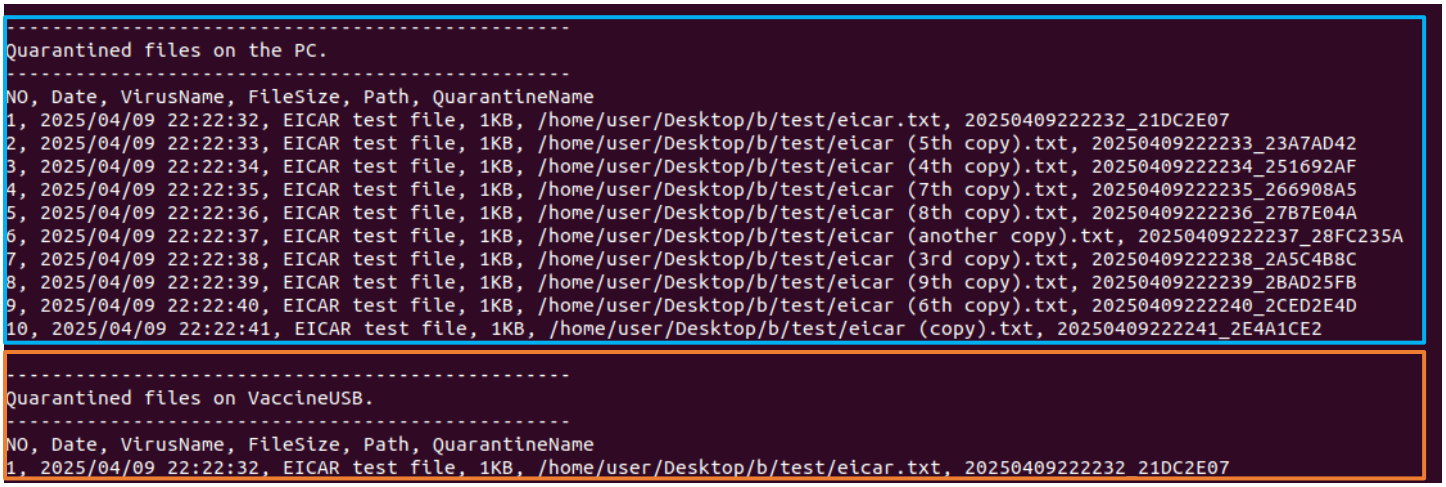
Caution: Do not directly delete or copy quarantine files yourself.

Quarantine File Management Command List

Action	Command
List quarantined files on PC and VaccineUSB	**-qt-list**
Copy quarantined files from PC to Vaccine USB Use when moving files to another PC for analysis	**-qt-list --to-usb**
Restore quarantined files on PC	**-qt-list --restore**
Delete quarantined files on PC	**-qt-list --delete-pc**
Delete quarantined files on Vaccine USB	**-qt-list --delete-usb**

List Quarantined Files

Item	Content
Function	Displays a list of quarantined files on the PC and VaccineUSB
Command Structure	**startuplnx.sh -qt-list**



Quarantined Files Information on PC

Field	Description
NO	Quarantine file number. This number is used to control the quarantined file.
Date	Date and time when the file was quarantined.
VirusName	Name of the malware.
FileSize	Size of the malware.
Path	Location where the malware was detected.
QuarantineName	Quarantined file name

Quarantined File Information Copied to Vaccine USB and Stored on Vaccine USB

Field	Description
NO	Quarantine file number. This number is used to control the quarantined file.
Date	Date and time when the file was quarantined.
VirusName	Name of the malware.
FileSize	Size of the malware.
Path	Location where the malware was detected.
QuarantineName	Quarantined file name

*Quarantined files within the Vaccine USB are stored in a hidden area of the Vaccine USB; therefore, they cannot be accessed from anywhere other than the Vaccine USB software.

Copy Quarantined Files from PC to Vaccine USB

Item	Content
Function	Copies quarantined files from the PC to Vaccine USB. Used when moving quarantine files to another PC for analysis. *Quarantined files within the Vaccine USB are stored in a hidden area of the Vaccine USB, therefore they cannot be accessed from anywhere other than the Vaccine USB software.
Command Structure	**startuplnx.sh -qt-list --to-usb --no:X**
Arguments (Options)	**--to-usb**: Copies all quarantined files from the PC to Vaccine USB. **--no:X:** To copy individual quarantined files from the PC to Vaccine USB, use this option and specify the quarantine file number (X). Check the file number with the [Command: List Quarantined Files].
Command Example	Copy all quarantined files from PC to Vaccine USB **startuplnx.sh -qt-list --to-usb** Copy quarantine file number 2 from PC to Vaccine USB **startuplnx.sh -qt-list --to-usb --no:2**

Restore Quarantined Files on PC

Item	Content
Function	Unzips quarantined files on the PC and restores them to their original locations. The quarantined file is deleted after restoration.
Command Structure	**startuplnx.sh -qt-list --restore --no:X**
Arguments (Options)	**--restore**: Unzips all quarantined files on the PC and restores them to their original locations. **--no:X:** To restore individual quarantined files on the PC, use this option and specify the quarantine file number (X). Check the file number with the [Command: List Quarantined Files].
Command Example	Unzip and restore all quarantined files on PC **startuplnx.sh -qt-list --restore** Unzip and restore quarantine file number 1 on PC **startuplnx.sh -qt-list --restore --no:1**

Delete Quarantined Files on PC

Item	Content
Function	Deletes quarantined files on the PC.
Command Structure	**startuplnx.sh -qt-list --delete-pc --no:X**
Arguments (Options)	**--delete-pc**: Deletes all quarantined files on the PC. **--no:X:** To delete individual quarantined files on the PC, use this option and specify the quarantine file number (X). Check the file number with the [Command: List Quarantined Files].
Command Example	Delete all quarantined files on PC: startuplnx.sh -qt-list **startuplnx.sh -qt-list --delete-pc** Delete quarantine file number 3 on PC **startuplnx.sh -qt-list --delete-pc --no:3**

Delete Quarantined Files on Vaccine USB

Item	Content
Function	Deletes quarantined files on Vaccine USB.
Command Structure	**startuplnx.sh -qt-list --delete-usb --no:X**
Arguments (Options)	**--delete-usb**: Deletes all quarantined files on Vaccine USB. **--no:X:** To delete individual quarantined files on Vaccine USB, use this option and specify the quarantine file number (X). Check the file number with the [Command: List Quarantined Files].
Command Example	Delete all quarantined files on Vaccine USB **startuplnx.sh -qt-list --delete-usb** Delete quarantine file number 5 on Vaccine USB **startuplnx.sh -qt-list –delete-usb --no:5**

12 Support

Support & Maintenance Contents

Item	Details
Product	VaccineUSB3
Support Content	Technical Support: Assistance with both the malware scanning software and hardware-related issues. Virus Definition Updates: Regular updates to ensure the virus database is current and effective against the latest threats. Software Enhancements: Minor updates to the malware scanning software, providing improved performance, bug fixes, and new features as needed.
Support / Warranty Period	ULD-VAU31A / HUD-MVDT31A: 1 year after purchase ULD-VAU33A / HUD-MVDT33A: 3 years after purchase ULD-VAU35A / HUD-MVDT35A: 5 years after purchase *Hardware warranty period starts from product delivery date

Contact Information:

Contact	
E-mail	vsolsupport@hagisol.co.jp

-This product incorporates "UDRW Technology," a USB storage technology combining CD-ROM and removable storage areas (patented):

Japan: Patent No. 3914949, Patent No. 3699717, Patent No. 3513147

U.S.A.: Patent No. 7,111,121 B2

China: Patent No. ZL200410038475.6

Hong Kong: Patent No. HK1068990 B

Taiwan: Invention Patent No. I 261757

Korea: Patent No. 589521

European Patent: (Italy, France, Germany, United Kingdom) Patent No. 149182

-Product specifications, appearance, and service contents are subject to change without prior notice. Thank you for your understanding.

-Third-Party Library Notice

This software uses GNU libstdc++ (libstdc++.so.5). GNU libstdc++ is distributed under the terms of GNU General Public License version 2 with the "Runtime Library Exception. The full text of the GNU GPL can be obtained from the following URL:https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

How to Obtain the Source Code

The source code for GNU libstdc++ is provided as part of GNU GCC (GNU Compiler Collection). It can be obtained through the following methods:

GNU GCC Official Website:

https://gcc.gnu.org/pub/gcc/releases/

*Note: libstdc++.so.5 is included in the gcc-3.2.x series

GNU FTP Mirror:

https://ftp.gnu.org/gnu/gcc/

User Rights

Under the GNU GPL, users are guaranteed the following rights.:

The right to obtain and modify the library source code

The right to relink this software using a modified version of the library

This software is designed to allow users to relink with newer versions of libstdc++. For information about relinking procedures, please contact us.

Note: This software uses libstdc++ as a dynamic link library. The license of this software itself is not affected by the libstdc++ LGPL license.

VaccineUSB3 Linux Version Software Manual

Published: April 2025

Publisher: Hagiwara Solutions Co., Ltd.