



DriveLock Release Notes

Release Notes 2024.2 Patch 2

DriveLock SE 2025




Table of Contents

1 DRIVELOCK RELEASE NOTES 2024.2 PATCH 2	4
1.1 Patch version 2024.2 Patch 2	4
1.1.1 Bug fixes	4
1.2 Patch version 2024.2 Patch 1	6
1.2.1 New features and changes	6
1.2.2 Bug fixes	6
1.3 Major version 2024.2	9
1.3.1 New features, improvements and changes	9
1.3.2 Bug fixes	11
1.4 Known issues and notes	17
1.4.1 BitLocker Management	17
1.4.2 BitLocker To Go	19
1.4.3 Data masking	19
1.4.4 Device Control	19
1.4.5 Disk Protection	21
1.4.6 DriveLock Enterprise Service (DES)	24
1.4.7 DriveLock Operations Center (DOC)	24
1.4.8 DriveLock Pre-Boot Authentication	25
1.4.9 Settings for enforced encryption	27
1.4.10 File Protection	27
1.4.11 Self-service	28
1.4.12 Thin Clients	28
1.5 End Of Life Announcement	30
2 SYSTEM REQUIREMENTS FOR OPERATING DRIVELOCK	33
2.1 DriveLock Agent	33
2.2 DriveLock Management Console	40

2.3	DriveLock Enterprise Service	40
2.4	DriveLock Operations Center (DOC)	42
3	SECURITY BULLETINS	43
3.1	Security Bulletin #22-001 - ZLIB external library vulnerability	43
3.2	Security Bulletin #22-002 - Log4net external library vulnerability	44
3.3	Security Bulletin #22-003 - DotNetZip.Semvered external library vulnerability	45
3.4	Security Bulletin #22-004 - Node.js external library vulnerability	46
3.5	Security Bulletin #22-005 - OpenSSL 3.0 external library vulnerability	47
COPYRIGHT	49

1 DriveLock Release Notes 2024.2 Patch 2

Build: 2024.2.4

Date: 2025-02-12

The DriveLock Release Notes contain important information about [bug fixes](#) and [known issues](#) in this patch version. They also contain an overview of the [system requirements](#) for using DriveLock, plus [end-of-life announcements](#). The new features and changes and the bug fixes in the main version are also included.

Please find a detailed description of the new features, improvements and changes in 2024.2 in the **What's new?** chapter. in the DriveLock documentation at [DriveLock Online Help](#).

Find the release notes of previous and still supported versions in the **Archives** menu at [DriveLock Online Help](#).



Please note the general information on updating to new versions in the **Updating DriveLock** chapter in the DriveLock documentation at [DriveLock Online Help](#).

1.1 Patch version 2024.2 Patch 2

1.1.1 Bug fixes

DriveLock 2024.2 Patch 2 is a patch version.

This chapter contains information on errors that have been fixed with DriveLock version 2024.2 Patch 2. Our External Issues (EI) numbers, if available, serve as a reference.

 Warning: Please note that some issues may cause a change in product behavior when you install the update. Before updating, make sure to check your settings to see if your existing environment is affected. The issues are labeled with the following icon 

Reference	Application Control
EI-2889	If querying detailed information was necessary when starting a binary (*.exe or *.dll) and this failed, this error was also cached for future program starts. Now, this is not the case anymore, so that a new execution of the file usually works.

Reference	Application Control
	Start times for processes in the process tree are now displayed correctly.

Reference	Device Control
EI-2885	The "Disable locked devices in device manager" setting works correctly again.
EI-2885	Under certain unknown circumstances, Windows failed to load the device control driver on some systems, even though it had been loaded successfully several times before. The issue has been fixed for some of these cases, but not all. In some cases, changing the setting to disable devices instead of blocking them may also help.
	<p>Extraction of allowed files from Zip Archives may have been incorrectly blocked in previous versions. In these cases, empty files were created in the target folder.</p> <p>Generally speaking, all writes under Content Scan Control may have produced problems if they were paging I/O (with size and buffer adjusted to disk access and not to real file sizes). This bug is fixed.</p>

Reference	DriveLock Agent
EI-2882	Drivelock drivers now work again under Windows 7.

1.2 Patch version 2024.2 Patch 1

1.2.1 New features and changes

In addition to the bug fixes, you will find the following changes in version 2024.2 patch 1:

- DriveLock now also supports media that have been checked by OPSWAT data gateways.
- DriveLock only supports case-insensitive database collations. (Reference EI-2848)

1.2.2 Bug fixes

DriveLock 2024.2 Patch 2 is a patch version.

This chapter contains information on errors that have been fixed with DriveLock version 2024.2 Patch 2. Our External Issues (EI) numbers, if available, serve as a reference.

Reference	BitLocker Management
EI-2788	A USB stick encrypted with BitLocker To Go was already accessible before the Defender scan was completed.

Reference	Device Control
	With setting "Block password-protected archives" NOT set, rar archive scanner did not block forbidden file extensions in password protected archives. This bug was introduced with 24.2 and is fixed now.
	WinZip AES compatible encrypted archives are now detected as password-protected archives too. In previous versions this worked for old Zip 2.0 encryption only.
	The restrictions for drive rules in DriveLock computer groups now work again for Linux and mac agents.


Reference	Device Control
	Since version 24.1, the hash calculation and the creation of shadow files sometimes failed if the file being processed was closed prematurely. This issue has been fixed.

Reference	Disk Protection
EI-2834	The challenge/response code for the PBA emergency login without user name remained the same after use if the SSO policy was disabled.

Reference	DriveLock Database
	Fixed an error in the database update to 24.2 if the database contained deleted DFP folder/user data that had not been properly removed.

Reference	DriveLock Operations Center (DOC)
EI-2827	The new dialog for displaying the old policy versions always showed only the latest 100 versions.
EI-2839	In the DOC, not all relevant computers were displayed under "Encryption" – in particular, the ones that were only licensed for File Protection were missing. In addition, many encryption events were missing there, namely all of them for Disk Protection, File Protection, BitLocker and BitLocker To Go.

Reference	DriveLock Operations Center (DOC)
EI-2830	It was not possible to add elements to empty groups or empty policy collections because the rights had not been checked correctly. The issue only occurred in combination with the assignment of rights to specific groups/policy collections. As long as the user had global rights to manage groups/policy collections, there were no issues.

Reference	Encryption 2-Go
 EI-2845	Changed behavior: The agent user interface no longer automatically uses the administrator password if no enforced encryption is configured or no enforced encryption rule is assigned.

Reference	File Protection
	The bug that prevented the automatic mounting of encrypted folders when they were accessed via 32-bit applications has been fixed.

Reference	Vulnerability scan
	Vulnerability CVE-2024-43483 related to .NET has been fixed.

1.3 Major version 2024.2

1.3.1 New features, improvements and changes

Below you will find a list of the new features, improvements and changes contained in version 2024.2

A detailed description can be found in the chapter **What's new?** in the DriveLock Online Help at [DriveLock Online Help](#).

Device Control

- End users can request approvals for composite and MTP devices
- Administrators can configure drive classes in the DOC
- Quick management and export of drive and device rules
- Management of drives in remote sessions on non-terminal servers
- Extension of the usage policy and SB release: Users can now use names in UPN format (name@domain)
- Content scanner event: Display of file headers for blocked files
- Extend archive scanning to encrypted containers and SMB shares
- Show hardware information in event columns
- Enable simulation mode for individual device classes
- Temporarily disable Defender scans during remote unlock

New system groups and modified group evaluation

- ⚠ DriveLock now introduces system groups that automatically include all computers or all users.

macOS

- Encrypt USB drives on macOS with Encryption 2-Go
- Quickly access encryption and recovery features with the Notifier for macOS
- Distribute the mac Agent via MDM

Linux

- AlmaLinux is supported as a new Linux distribution on endpoints
- Extend Device Control on Linux to support vendor and product information

Application Control

- Manage Application Behavior Control rules in the DOC
- Improve the display and settings for Application Control rules in the DOC
- Simplify process analysis with the process tree

BitLocker Management

- Automatically encrypt devices during provisioning with TPM

DriveLock Operations Center

- Use dark mode, customize list views, perform central searches, and more
- Evaluate, distribute, and modify licenses, and create license policies
- Evaluate licenses on a tenant basis for managed service environments

General improvements and changes

- Manage endpoints and groups via the platform API
- Automatically delete inactive computers from the inventory
- Centrally manage encrypted folders
- Integrate risk assessments and training with Human Risk Assessment & Security Awareness
- The login screen behavior for DriveLock PBA is aligned with Windows
- Use the new DriveLock Server Installation Wizard for database installation and server certificate management (replacing the older tools Database Install Wizard.exe and ChangeDesCert.exe)
- Allow the DriveLock Enterprise Service to use a group-managed service account (gMSA) as a login account.

System requirements update


- In addition to .NET Framework 4.8, the DriveLock Enterprise Service now requires [.NET Core 8.0 Runtime](#)


1.3.2 Bug fixes

DriveLock 2024.2 is a major version.

This chapter contains information on errors that have been fixed with DriveLock version 2024.2. Our External Issues (EI) numbers, if available, serve as a reference.




Warning: Please note that some issues may cause a change in product behavior when you install the update. Before updating, make sure to check your settings to see if your existing environment is affected. The issues are labeled with the following icon .



	Application Control (AC)
	<p>Filters for application behavior control and application lists ending with a backslash, followed by wildcards, incorrectly matched files in child directories. For example, <code>c:\test*</code> matched <code>c:\test\sub-dir\readme.txt</code>. To match all files in all child directories, the filter must be <code>c:\test\</code> or <code>c:\test***</code>.</p> <p>This is a behavior change: filters are now evaluated correctly!</p>
	<p>If application behavior rules were saved in the DMC without selecting the 'Filters' tab, command line parameters were not saved, and changes to the target were not applied.</p>
	<p>The timing of rule evaluations has been improved to prevent longer-running checks from slowing down others.</p>

	BitLocker Management (BLM)
	<p>When decrypting BitLocker-encrypted partitions, events were sent without specifying any data. This resulted in an error message in the DES log file.</p>

	BitLocker Management (BLM)
	The menu item "Encryption" in the DOC Security Controls was not displayed if you only had BitLocker licensed.
EI-2787	When restricting the BitLocker password to numbers or numbers and Latin letters, dictionary files could not be used because the option was grayed out.
	After resuming a delayed encryption, it was possible that external hard disks were also encrypted.
EI-1611	The uninstallation of the DL-PBA was incomplete under certain circumstances, despite the corresponding assigned policy, making it impossible to uninstall the DriveLock Agent.

	Defender Management
EI-2790	Fixed an issue with transmitting the detected threats to the DES.

	Device Control
	Fixed an issue that made the content search for files in rar archives unreliable.
	If the 'Allow authorized user login' option is enabled for a usage policy, the currently logged in user can only accept the usage policy (without specifying another account) if they are also listed in the list of authorized users.

	Device Control
	This is a change in behavior. If the logged-in user is to be able to accept the usage policy, they must be entered in the list via the 'Authorized users' option.
	<p>If the usage policy is configured with the option 'Launch self-service unlock after accepting usage policy', but the accepting user does not have authorization for self-service unlock, the usage policy can now simply be accepted without starting the self-service unlock.</p> <p>This is a change in behavior. If you want to specify users who are allowed to accept the usage policy, you can enter them in the list using the 'Authorized users' option.</p>
EI-2682	In the DMC, when browsing for COM ports (Devices -> Device class locking -> Serial ports (COM) -> Ignored port devices), the ports available locally (or on an agent connected via remote control) were not listed. PCMCIA adapters would have been displayed instead, if available.
	The Linux agent can now be installed on the SUSE Enterprise desktop.
	<p>The Linux Agent now reports composite devices with the correct hardware ID for all interfaces.</p> <p>Please check your already configured device rules and use wild-cards (*) to map all interfaces of a device, e.g.: USB\VID_1234&PID_1234&REV_0001*.</p>

Reference	Disk Protection
	Fixed an issue in the user-related agent settings where the display of Disk Protection logon notifications did not work correctly.
	A successful emergency pre-boot logon (event 503) was not logged.

Reference	DriveLock Agent
	The settings for the push installation of the agent via a linked DES were read from the central DES.
EI-2779	The content scanner has blocked some valid DOCX files.
EI-2768	It was not possible to control external drives with serial numbers on the macOS Agent.
	In some configurations, the agent sometimes tried to start a blocked device, which led to unnecessary events.

Reference	DriveLock Enterprise Service (DES)
	The maintenance settings of clients are now correctly evaluated per client.
EI-2678	A scheduling problem in connection with summer time has been fixed.

Reference	DriveLock Management Console (DMC)
EI-2726	Events 704-706 have been moved to a more appropriate event category (Device events instead of Temporary unlock).
EI-2709	The option to select a file from the application inventory was also offered if no application inventory was available.
	If a policy in the new format was created with a policy in the old format as a template, the new policy was empty.
	Removing the default restore settings from a policy did not work.

Reference	DriveLock Operations Center (DOC)
EI-2777	In the DOC, any duplicate spaces in the event properties were replaced with a single space in the parameters, so that after copying and pasting, for example, ProductIDs, they could not be used correctly in rules.
EI-2720	In the detail view of computers, the "Definition" tab in the "Group memberships" window has been renamed "Static group definitions" to avoid confusion.
EI-2772	An error in the listing and correct counting of objects has been fixed. This error could occur with restricted DOC user authorizations (for OUs or groups).
	Under certain circumstances, taking over a report from another

Reference	DriveLock Operations Center (DOC)
	user could lead to a loss of the report settings.
EI-2750	Notifications in the DOC did not work for third-party events, although they could be configured.

Reference	DriveLock Setup
EI-2640	On Windows servers, some Windows files remained changed after uninstalling the DriveLock Agent when MTP device control was enabled.

Reference	Encryption 2-Go
EI-2714	The length of the entered drive label for enforced encryption was not checked. As a result, the encryption process could not be completed when more than 11 characters were assigned.

Reference	File Protection (FFE)
	Compatibility problems occurred when locking regions of files on network shares. For more information, see the known issues and notes for File Protection.

1.4 Known issues and notes

1.4.1 BitLocker Management

Supported versions and editions:

DriveLock BitLocker Management supports the following operating systems:

- Windows 7 SP1 Enterprise and Ultimate, 64 bit, TPM chip required
- Windows 10 Pro and Enterprise, 32/64 bit
- Windows 11 Pro and Enterprise, 64-bit

Native BitLocker environment

Since version 2019.1, if you want to manage an existing system environment that already contains computers encrypted with BitLocker, they no longer need to be decrypted beforehand via the existing BitLocker management or group policies. DriveLock detects native BitLocker encryption automatically and creates new recovery information. The drives are only decrypted and encrypted automatically if the encryption algorithm configured in the DriveLock policy differs from the current algorithm.

After that, you can use DriveLock BitLocker Management to manage your computers and securely store and utilize the recovery information.

Using passwords

With DriveLock BitLocker Management, the misleading distinction between PINs, passphrases and passwords is simplified by simply using the term "password". Also, this password is automatically used in the correct BitLocker format, either as a PIN or as a passphrase.

Since Microsoft has different requirements for the complexity of PIN and passphrase, the following restrictions apply to the password:

- Minimum: 8 characters. In some cases, you can also enter 6 characters (numbers); for more information, see the Password options chapter in the current documentation at [DriveLock Online Help](#).
- Maximum: 20 characters



Warning: Note that BitLocker's own PBA only provides English keyboard layouts, which means that using special characters as part of the password may cause login issues.

Encryption of external hard disks

Microsoft BitLocker limitations prevent external hard disks (data disks) from being encrypted if you have selected the "TPM only (no password)" mode, since BitLocker expects you to enter a password (BitLocker terminology: passphrase) for these extended drives.

Encryption on Windows 7 agents

On Windows 7 agents, the following error may occur when you use the new execution options added in DriveLock 2020.2: BitLocker does not encrypt on Windows 7 if the "when the screen saver is configured and active" and "when no application is running in full screen mode" options are enabled.

Moving from Disk Protection to BitLocker Management

You must remove Disk Protection with the appropriate policy setting before you can use BitLocker Management.

1.4.2 BitLocker To Go

Encryption with BitLocker To Go

- After encrypting a USB stick with an administrative password, it would not connect. To solve the issue, remove the USB flash drive first and then plug it back in.

Enforced encryption with BitLocker To Go

- With enforced encryption (BitLocker To Go), unencrypted access is only possible until the next configuration update.

1.4.3 Data masking

Data masking on macOS

- Please note that data masking is not yet implemented for the macOS agent.

1.4.4 Device Control

Drivers for device control

- Under certain unknown circumstances, Windows may fail to load the device control driver on some systems, even though it has been loaded successfully several times before. The issue has been fixed for some of these cases, but not all. In some situations, it may also help to change the setting so that devices are disabled instead of blocked. (Reference EI-2885)

Quota / File filter templates

- On the Quota tab, the bytes written or read per time unit are counted, not the actual files. Therefore, the creation of new files with 0 bytes is not blocked.
- Each opened file counts towards the number, even for the same file, and sizes are accumulated.
- The read quota has priority over the write quota, as a read operation is required before the write operation and is blocked if the read quota has already been exceeded.
- The behavior of quoting is application-specific and depends on how an application opens a file for what appears to be a simple read or write request from the user. A file can be cached or opened multiple times or duplicated or renamed before the actual read/write processing, e.g. Wordpad consumes the number of files by 3 each time it is opened. Interfering processes acting on behalf of the user (AV) may further falsify the planned behavior

File filter for archive files

- If a file excluded in the file filter is copied to an archive file, the entire archive file is deleted. We recommend that you do not edit archive files directly on the controlled volumes, but on the local hard disk, where no file filter is usually set. (Reference EI-2651)
- Using Content scanning for archives may produce a high event load, in particular for Event 133 "File accessed".
One reason for this may be having installed the Shell Extensions of the archive programs
- Please note the following information:
 - Nonstandard application behavior may lead to unexpected results, e.g. 7zip opens the zip and shows sections of a forbidden exe in analysis mode
 - WebDAV drives are still not supported
 - Hash exclusions are not applied within archives
 - Simulation mode does not include content scanning
 - If an archive is blocked and initial action was a move from an unfiltered location, the source in the unfiltered location is currently deleted as well. (Reference DL-7643)

Please also note that

- archives can be scanned up to a nesting level of 2, i.e. zip1/zip2 is scanned, but zip1/zip2/zip3 is blocked,
- size/number of contained files are not limited; therefore, in spite of a variable timeout adapted to compressed size, a timeout may occur during the scan
- archive scans on large archives (several GB) may fail: Archives cannot be opened and/or the scan may cause Drivelock to crash.
- timeouts and other failures, e.g. failure to open the archive for scanning for whatever reason, will not lead to blocking access.

Long serial numbers

- Drives with serial numbers longer than 63 characters cannot be blocked or allowed by a whitelist rule with a required serial number or a default policy.

Files blocked for a short time

- Files may be blocked on a USB flash drive for short time during a configuration update when a file filter is configured and access is permitted for specific users or groups.

Cumulative Windows Server 2022 Security Updates on Terminal Server

- Please take the following manual steps if you continue to encounter errors on the affected Windows servers after installing or updating the DriveLock Agent: (Reference EI-2639)
 - **If MTP control is activated:**

Stop the DriveLock Agent Services and the DriveLock Health Monitor (e.g. `net stop drivelock & net stop dlhm`) before installing the Windows update. They will be restarted automatically after the reboot.
If necessary, restart DriveLock manually if it does not restart automatically.
 - **If MTP control is not activated:**

After updating from an older DriveLock Agent version, please execute the following commands once in the command line: `drivelock -regmtpfltnf` and `drivelock -unregmtpfltnf`.

CD-ROM drives

- DriveLock only shows a usage policy once when a CD is inserted. When ejecting the CD and inserting a new one, the usage policy does not appear any more but the new CD is blocked nonetheless. When you restart DriveLock, the usage policy appears again.



Note: This is because DriveLock only recognizes the actual device in the policy (CD-ROM drive), not the content (CD-ROM).

1.4.5 Disk Protection

Important information

Disk Protection is no longer supported for Windows 7 or older (missing BIOS support, see [EoL announcements](#)).

Windows Inplace Upgrade

If you have activated a certain number of automatic logins for the PBA before updating to a current Windows 10 version (`dlfdecmd ENABLEAUTOLOGON <n>`), the automatic login is active throughout the upgrade process. However, since the `<n>` counter cannot be updated during the process, we recommend that you just set it to 1 so that after upgrading, after another reboot, there is only one automatic login followed by another user login to the PBA.

Antivirus software

Antivirus protection software may cause the DriveLock Disk Protection installation to fail if the antivirus software quarantines files in the hidden `C:\SECURDSK` folder. If this occurs, please disable your antivirus protection for the duration of the Disk Protection installation. We recommend that you configure your virus scanner with an exception for the folder.

Application Control

We strongly recommend that you deactivate Application Control, if it is active in whitelist mode, for the duration of the Disk Protection installation to prevent programs required for the installation from being blocked.

Hibernation

Hibernation will not work while a disk is encrypted or decrypted. After complete encryption or decryption windows has to be restarted once to make hibernate work again.

UEFI mode



Note: Not all hardware vendors implement the complete UEFI functionality. You should not use the UEFI mode with UEFI versions lower than 2.3.1.

- DriveLock PBA is designed for Windows 10 and 11 because the driver signatures required for the full disk encryption components are only valid for these operating systems.
- The PBA for UEFI mode may cause issues with PS/2 input devices (e.g. built-in keyboards).
- With VMWare Workstation 15 and also with a few hardware manufacturers, our test results revealed conflicts with mouse and keyboard drivers of the UEFI firmware, so that keyboard input in the PBA is not possible. In this case, you can use the "k" key to prevent the DriveLock PBA drivers from loading once when you start the computer. After Windows logon to the client, you can then run the `dlsetpb /disablekbddrivers` command in an administrator command line to permanently disable the DriveLock PBA keyboard drivers. Be aware that the standard keyboard layout of the firmware is loaded in the PBA login mask, which usually is an EN-US layout, so special characters may differ.

Introducing the combined driver as of version 2020.1 solves the issue on some systems (including VM Ware Workstation 15).

For more information, please refer to the Shortcut and function keys in the DriveLock documentation at [DriveLock Online Help](#).

Note the following information:

- DriveLock 7.6.6 and higher supports UEFI Secure Boot.
- If you update the firmware, the NVRAM variables on the mainboard that DriveLock requires may be deleted. We recommend that you install the firmware updates for the mainboard / UEFI before installing the DriveLock PBA / FDE (also for newly purchased devices or bug fixes).
- A 32 bit Windows operating system or 32 bit DriveLock cannot be installed on 64 bit capable hardware. Please use a 64 bit version of a Windows operating system and DriveLock instead.
- There is still a limitation to disks up to a maximum of 2 TB disk size.
- Some HP computers always have Windows in position 1 of the UEFI boot order and the DriveLock PBA has to be selected manually in the UEFI boot menu. In this case fast boot has to be switched off in UEFI to keep the DriveLock PBA at position one.

1.4.6 DriveLock Enterprise Service (DES)

Registration of linked DES

A linked DES can only be registered if the user has not activated multi-factor authentication (MFA).

1.4.7 DriveLock Operations Center (DOC)

⚠ Adjusted role permission checks on groups and policy collections

Role permissions for groups are now checked within the context of the specific group or OU. Previously, it was possible to add or remove computers in any group, even if the user only had permissions for a specific group or OU. In version 2024.2, the permission checks have been adjusted to respect restrictions to the assigned group or OU. To grant permissions across all groups or OUs, use the global "Manage Groups" permission.

The same applies to policy collections, where the "Manage Policy Collection" permission is now checked accordingly.

Old versions of DOC.exe are no longer supported

You will need to manually uninstall old DOC.exe versions starting with version 2021.2. Note that these old versions will no longer work with an updated DES and are therefore discontinued.

Login to the DOC for users who have been removed from an AD group

Logging on to the DOC continues to work even if the user has already been removed from an AD group and therefore no longer has authorization to log on to the DOC. This is because group memberships for a user are read from the group token. This information is only updated at certain intervals.

Logging in with Windows authentication for users in the 'Protected Users' group

- It is not possible to log in to the DOC using Windows authentication if a user belongs to the "Protected Users" security group. However, logging in via a password works here.
- It is also not possible to log in to the DOC via Windows authentication if users have logged in to Windows with a smartcard. At present, this is not supported. (Reference EI-2597)

1.4.8 DriveLock Pre-Boot Authentication

- Hardware must support the TCP4 UEFI protocol for the DriveLock PBA network functionality to work. For this reason, some systems may run into trouble if the UEFI BIOS does not support the required network connections. This is specifically the case with the following systems:
 - Fujitsu LifeBook E459. (Reference: EI-1303)
 - Fujitsu LifeBook U772
 - Acer Spin SP11-33
 - Acer Spin SP513-53N
 - Dell Inspiron 7347
- The UEFI firmware of guest systems in Hyper-V environments does not supply the Microsoft Corporation UEFI CA 2011 certificate, which is mandatory for using DriveLock PBA on Hyper-V clients with SecureBoot enabled. Therefore, the DriveLock PBA is presently not supported on Microsoft Hyper-V clients. (Reference EI-2194)
- The EURO character "€", that a German keyboard provides when entering the 'Alt Gr' and 'e' combination, is not recognized when logging into the DriveLock PBA.
- On some DELL devices, the implementation of time counting differs from the standard and may result in a longer time span than expected. Unfortunately, we cannot solve this hardware-related issue through programming. (Reference: EI-1668)
- DriveLock uses its own UEFI driver for keyboards by default (either a simple one or a combination driver with mouse support) to offer international keyboard layouts within the PBA as well. It is loaded with the help of a UEFI standard interface. On some models, this interface specified in the UEFI standard is not implemented correctly or not at all. In such cases, it is possible to disable loading the DriveLock driver, either using the command line command "dlsetpb /KD-" or via a setting within the policy available in DriveLock version 2021.2.
Note that the default driver implemented by the manufacturer is used here, which usually only supports an English keyboard layout.
- If you add additional unencrypted disks to an already encrypted system, always make sure to access the new disks after the existing disks to avoid any access issues to the EFS or failure to synchronize users. (Reference: EI-1762)
- When the PBA is installed, the Windows logon screen provides logon for other users, but does not show the user who was logged on last time. This occurs because of the

"Fast User Switching" feature used for that purpose in Windows and its implementation by Microsoft. (Referenz: EI-1731)

- Warning: In the event of a time change (for example, winter time to daylight saving time), you run into a mismatch between server and system time if your DriveLock Agents were shut down prior to the change (thus using the 'old' time), but the time on your server has already been changed. In this case, the login to the network PBA is blocked. End users must select a different logon method once (user name / password entry) or you need to adjust the system time manually. Once both times are synchronized, logging into the network PBA will work again. (Reference EI-1817)
- The DriveLock PBA requires smart card readers to have a CCID V1.1 compliant interface.

1.4.9 Settings for enforced encryption

Setting the encryption method for forced encryption of an external storage device

- If the administrator did not specify the encryption method, a dialog for selecting the encryption method (Encryption-2-Go, Disk Protection, BitLocker To Go) appears on the DriveLock agent when connecting the external storage device. In some cases, however, this dialog appears incorrectly even for SD card readers without media.

1.4.10 File Protection

Microsoft OneDrive

- With Microsoft OneDrive, Microsoft Office may synchronize directly with OneDrive instead of writing the file to the local folder first. Then the DriveLock encryption driver is not involved and the Office files will not be encrypted in the Cloud. To stop this behavior, deselect **"Use Office 2016 to sync files I open"** or similar settings in OneDrive. Make sure that Office files as other files always are stored locally.
- Deleting encrypted folders in the local OneDrive directory can, under certain circumstances, result in an empty folder remaining.

FireEye

- The FireEye product may trigger a blue screen error (BSOD).

NetApp

- Currently, some incompatibility persists between DriveLock's encryption driver and certain NetApp SAN drivers or systems that cannot yet be more precisely defined. Please check the functionality you require before using File Protection in this system environment. We are happy to help you here to analyze the issue in detail if necessary.

Windows 10 clients with Kaspersky Endpoint Security 10.3.0.6294

- Using File Protection in new format (PFE) and Kaspersky on the same system can lead to a blue screen error (BSOD), depending on which settings are used in the AV software. (Reference EI-2524)

Accessing encrypted folders

- Access to encrypted folders on drives that are not mounted with drive letters but as volume mountpoints is not supported.

Copying data to a network folder encrypted with a new format

- The blue screen error (BSOD) MUP_BUGCHECK_NO_FILECONTEXT may occur when copying 20-40 MB to an encrypted network folder. (New format, automatic mode) (Reference EI-2684)

Locking file regions on network shares

- To resolve potential compatibility issues with certain programs, starting from version 2024.2, the setting 'Files on network shares for which file region locks are not modified' can be used as a workaround.

File Protection and USB drives

- You cannot use DriveLock File Protection to fully encrypt a connected USB drive if the drive already contains an encrypted folder. In this case the following message appears "Cannot read management information from the encrypted folder".
- In case a removable storage device (USB stick) is encrypted, removing the device may make it impossible to open the folder that was just encrypted. If the device is formatted and reconnected externally when this happens, a new initial encryption that follows may be stuck due to the previous deactivation error.
If this type of workflow is wanted, we recommend either disconnecting the folder before removing it or removing the device "safely" (e.g. by ejecting it) and allowing for possible rejection, i.e. closing open files.

Check for unencrypted files

- If the 'CheckForUnencryptedFiles' function finds unencrypted files in network folders after a successful mount, the subsequent initial encryption of these files fails.
We recommend canceling the process, then unmounting and remounting the folder.
The check and initial encryption is successful in this second run.

Distributed File System (DFS)

- DriveLock File Protection supports storing encrypted directories in the new format on network drives with Distributed File System (DFS). DriveLock File Protection basically also supports storing encrypted directories on a network drive with Distributed File System (DFS). Since DFS and the associated storage system can contain customer-specific characteristics, however, we recommend that you test encrypted directories in detail before using them.

1.4.11 Self-service

If you are using the self-service wizard to unlock Apple iPhone devices, it is still possible to manually copy images from the iPhone device after the unlock is complete, as long as the device is connected.

1.4.12 Thin Clients

Please note the following restrictions when using DriveLock and Thin Clients:

- Security Awareness cannot be used on IGEL clients.

1.5 End Of Life Announcement

DriveLock sends out a newsletter in time to inform you about the end of support and maintenance for a specific DriveLock version.

For the following versions, the corresponding End-Of-Life (EoL) data apply:

Version	On-premise customer support exists until:	Cloud customer support exists until:
All versions before 2022.2	EoL - not supported any more	EoL - not supported any more
2022.2	June 2025	EoL - not supported any more
2023.1	Development support ^{*1} : December 2024 Product support ^{*2} : June 2025	EoL - not supported any more
2023.2	Development support ^{*1} : June 2025 Product support ^{*2} : December 2025	EoL - not supported any more
2024.1	Development support ^{*1} : December 2025 Product support ^{*2} : June 2026	Until the release of a version following 2024.2
2024.2	current version	current version



Note: We recommend that all our customers install the latest DriveLock version.

Support lifecycle:

Since version 2023.1, the support lifecycle for new DriveLock product versions is as follows: once a new product version is released, we announce the End-Of-Life (EOL) of the **previous version**.

*1 DriveLock will continue to provide full support for this version for 12 months from the date of the EOL announcement. This includes critical maintenance updates, code fixes for bugs and critical issues.

After the expiration of full support (12 months), DriveLock will no longer release new updates for this version.

*2 However, DriveLock product support is available for a further 6 months to answer telephone, e-mail and self-service inquiries.

This applies to all on-premise versions from version 2023.1.

Upgrades:

Customers who have previous product versions and a valid maintenance contract can upgrade the environment to the latest product version.

End of life of features:

- Version 2024.2 is the last version that supports policy signing certificates.
- With version 2024.2, Vulnerability Scan for Windows 8.x and older is no longer supported.
- With version 2024.2, BitLocker Management for Windows 8.x and older is no longer supported.
- With version 2024.2, the policy settings for the BIOS PBA no longer work on agents with version 2022.1. This means that the corresponding policies are completely removed and the continued operation of agents with BIOS PBA is therefore no longer possible.
- With version 2024.2, automatic push groups and OUs for the push installation of DriveLock agents are no longer supported. All other functions and settings of the push installation are already available in the DriveLock Operations Center, which is why the entire node will be removed from the DriveLock Management Console in ver-

sion 2024.2.

- With version 2024.2, the macOS Monterey operating system is no longer supported.
- The DriveLock Control Center (DCC) was only officially supported until May 2024 and has now been discontinued.




Note: **TLS 1.2:** Please make sure that all operating systems running DriveLock support TLS 1.2. as of now.

2 System requirements for operating DriveLock

The values listed in this document are recommended and represent minimum requirements. The requirements may vary depending on your configuration of DriveLock, its components and features, and your system environment.

2.1 DriveLock Agent

DriveLock Agent can be installed on different versions of Windows, Linux and macOS.

Operating system	Versions
Windows 11	As of 21H2, only Pro / Enterprise editions
Windows 10	As of 20H2, only Pro / Enterprise editions
Windows 10 LTSC	all LTSC versions until expiry of the respective Extended Support
Windows Server	2016, 2019, 2022
Windows 7	Windows 7 SP1 Enterprise / Ultimate with Extended Support. <div>  Note: An additional Legacy Support license is required when running on Windows 7 systems. </div>
Linux	Debian 12, Fedora 40, IGEL OS 11.05, Red Hat Enterprise Linux 5, SUSE 15.4, Ubuntu 24.04, AlmaLinux OS 9.4 or newer versions
macOS	From version Ventura (version 13) with Intel (x86_64) and Apple Silicon (arm64) architectures

The Windows DriveLock Agent is basically available for AMD-/Intel X86-based systems (32-bit and 64-bit architecture). We recommend using a 64 bit system for the DriveLock Agent.

Server operating systems are only supported under 64-bit. You will find the restrictions of the individual functionalities described below.



Warning: .NET Framework 4.7.2 is required to display security awareness campaigns on DriveLock Agents.

See the following table for an overview of the functionality available on a particular operating system.

Complete range of functions: ✓

Reduced range of functions: ◐

No support: ✗

Feature	Operating system / functions				
	Windows 10 / 11	Windows Server	Windows 7	Linux	Mac OS
Device Control	✓	✓	◐	◐	◐
Application Control	✓	✓	✓	◐	✗
Encryption-2-Go	✓	✓	✓	◐	◐
BitLocker To Go	✓	✓	◐	✗	✗
BitLocker Management	✓	✓	◐	✗	✗
Security Awareness Multimedia campaigns	✓	✓	✓	✗	✗
Defender Management	✓	✓	◐	✗	✗

Feature	Operating system / functions				
Vulnerability Management	✓	✓	✓	✗	✗
Security Configuration Management	✓	✓	✓	✗	✗
Disk Protection	✓(*)	✗	✗	✗	✗
File Protection	✓	✓	●	✗	✗

(*): On Windows 10 and newer, Disk Protection is available only for UEFI systems, BIOS support has been discontinued.



Note: Security Awareness: Please note that as of version 2022.1, Content AddOn packages can only be displayed correctly if Microsoft Edge WebView2 is installed on the agents. Please follow the download link: [https://developer-microsoft.com/en-us/microsoft-edge/webview2/#download-section](https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section). Windows 11 already has Microsoft Edge WebView2 installed automatically.



Note: As of version 2024.1, the latest Microsoft Visual C++ Redistributable is required for File Protection. To download the Redistributable, please click this [link](#).


Details on the restrictions for operating systems that can only use some of the DriveLock features:

1. Restrictions for Windows Server

- DriveLock pre-boot authentication is not available for server operating systems.
- Microsoft Defender settings are only available for Windows Server 2016 and later.

2. Restrictions for Windows 7

Make sure that the latest available patch level is installed on a Windows 7 client.

- In general:
 - After updating, installing or uninstalling DriveLock Agent on Windows 7 x64, the Explorer (explorer.exe) may crash. This only occurs if the Windows command prompt is opened with admin privileges and the system has not been rebooted since the agent was updated/ installed/uninstalled.
 - KB3140245 must be installed on Windows 7
Further information can be found under '[Update process](#)' and '[Update catalog](#)'.
Without this update, WinHTTP cannot change any TLS settings and the error 12175 appears in the dlwsconsumer.log und DLUpdSvx.log log files.
 - KB3033929 (SHA-2 code signing support) must be installed on Windows 7 64 bit.
 - DriveLock Service adds missing registry values for TLS 1.2 connections on computers running Windows 7.
The following registry values are the prerequisite for communication with the DES in addition to KB3140245:
 - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "Enabled"=dword:00000001
 - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "Enabled"=dword:00000001
 - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\WinHttp] "DefaultSecureProtocols"=dword:00000800
-  **Note:** If the DefaultSecureProtocols value already exists, add the value 0x00000800 for TLS 1.2.
- BitLocker Management:
 - Only available for Windows 7 SP1 Enterprise and Ultimate, 64-bit - TPM chip is required

- BitLocker does not encrypt on Windows 7 if the options "When the screen saver is configured and active" and "When no application is running in full screen mode" are enabled.
- BitLocker To Go:
 - Only available for Windows 7 SP1 Enterprise and Ultimate
- Device Control:
 - In Windows 7, you cannot use the Bluetooth options for devices in the Device class locking section.
- File Protection:
 - Under Windows 7, only the limited functionality is available for the new encryption format and only the previous legacy driver is available for the old encryption format. The appropriate encryption format is selected automatically.
- Security Awareness Multimedia Campaigns:
 - To be able to display Security Awareness multimedia campaigns you need a local installation of WebView2 for Windows 7. For more information, click here: <https://docs.microsoft.com/en-us/microsoft-edge/webview2/>

3. Restrictions for macOS

- Device Control:
 - No unlocking for specific users or user groups
 - No file filter and auditing
 - No unlocking for drives already encrypted with Encryption 2-Go
 - No self-service functionality
- Encryption 2-Go:
 - For macOS, the Mobile Encryption Application (MEA) is available as before for decrypting external USB drives.
 - The macOS agent can automatically encrypt drives with an Encryption 2-Go container, but the full functionality for Windows is not yet available.

For more information about the macOS agent, please refer to the macOS topics in the DriveLock online documentation.

4. **Restrictions for Linux**

- Device Control:
 - No unlocking for specific users or user groups
 - No file filter and auditing
 - No forced encryption
- Application Control:
 - DriveLock Application Control requires Linux kernel version > 5 for use on Linux agents.
 - Application Control cannot be used together with IGEL OS.
 - None of the Application Behavior Control functions are available on Linux.
- Encryption 2-Go:
 - Containers or encrypted USB drives cannot be created, only connected.

For more information on the Linux client and the limitations of its functionality, please refer to the Linux topics in the DriveLock online documentation.

5. **Restrictions for terminal server environments and thin clients**

- The DriveLock Agent requires the following system requirements in order to use the DriveLock Device Control functionality:
 - XenApp 7.15 or newer (ICA).
 - Windows Server 2016 or newer (RDP).
- Security awareness campaigns for users at login and ICA drive connections are not available when using thin clients without DriveLock Agent installed.

2.2 DriveLock Management Console

Before you install the DriveLock Management Console, please make sure that the computer meets all of these requirements to ensure full functionality.



Warning: Always use the DriveLock Management Console (DMC) that matches the DriveLock Enterprise Server (DES) version.

Main memory:

- at least 4 GB RAM

Free disk space:

- approx.350 MB

Additional Windows components:

- .NET Framework 4.8 or higher

Supported platforms:

The Management Console 2024.2 has been tested and released on the current levels of 64-bit Windows versions that were officially available at the time of release and that have not yet reached the end of the service period at Microsoft. Please check the [DriveLock Agent](#) chapter for a list of Windows versions that DriveLock supports.

2.3 DriveLock Enterprise Service



Note: This information applies only to DriveLock On-Premise installations.

Before distributing or installing the DriveLock Enterprise Service (DES) on your corporate network, please ensure that the computers meet the following requirements and are configured properly to provide full functionality.

Main memory / CPU:

- at least 8 GB RAM, CPU x64 with 2,0GHz and EM64T (Extended Memory Support)

Free disk space:

- at least 4 GB, with policies that do include Security Awareness campaigns with video sequences (Security Awareness Content AddOn), approx. 15 GB is recommended
- if the server is also running the SQL-Server database, additional 10 GB are recommended for storing DriveLock data

Additional Windows components:

- .NET Framework 4.8 or higher is required for installation!
- .NET 8.0 Runtime ([Microsoft Download Link](#))
- ASP.NET 8.0 Core Runtime([Microsoft Download Link](#))



Note: Depending on the number and duration of the DriveLock events that are stored, the size of the DriveLock database can vary greatly from one system environment to another. It is therefore difficult to provide an exact specification here. We recommend setting up a test environment with the planned settings over a period of at least a few days to determine the exact values. These values can be used to calculate the required memory capacity.

Required DriveLock Services ports:

Port	Usage
1883; 3004; 4370; 5370; 6369; 3003; 4567; 4766; 18083; 18084	These local ports must not be used by other server services. They are only used internally and do not have to be open externally.
8883	The agents connect to the DES on this port so that they can be accessed via remote agent control. The DES installation program automatically enables the clearance in the local firewall of the computer.
4568	This port is mainly used for the DriveLock Operations Center (DOC).
6066; 6067	These ports are used to transfer management and status information from the agents.

Supported platforms:

- Windows Server 2016 64-bit
- Windows Server 2019 64-bit


- Windows Server 2022 64-bit

On a Windows 10/11 client operating system, a DES should only be run as a test installation.

 Warning: The DES is only available as a 64-bit application.


Supported databases:

- DriveLock version 2024.1 or higher requires at least SQL Server 2016 SP1 or newer. The database must have a compatibility level of 130 or higher.
- SQL Server Express 2016 or newer for installations with up to 200 clients and test installations
- The DES requires the **Microsoft SQL Server 2012 Native Client version 11.4.7001.0**. In case this component is not yet installed, this happens automatically before the DES is actually installed. If an older version is already installed, it will be updated automatically.

 Note: Please refer to the applicable Microsoft documentation regarding the system requirements for installing the SQL database or SQL Express.

 Warning: The database connection between the DriveLock Operations Center and the database requires a TCP/IP connection.

2.4 DriveLock Operations Center (DOC)

 Note: This information applies only to DriveLock On Premise installations.

The web-based DriveLock Operations Center is included in the DES installation and is not a stand-alone component. It is accessed via a browser. The DriveLock Policy Editor can be accessed via DOC Companion.

SQL Server 2016 or newer is the minimum requirement for DriveLock Operations Center.

DriveLock Operations Center is only available for AMD / Intel X86 based 64-bit systems.

3 Security Bulletins

3.1 Security Bulletin #22-001 - ZLIB external library vulnerability

First published: **21th April 2022**

Last updated: **3rd June 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of the ZLIB library. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2019.2
- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

The detected vulnerability in ZLIB before version 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. DriveLock uses this library mainly to decompress previously packed files, which doesn't affect security due to the nature of this vulnerability.

The DriveLock Support Companion uses the library to pack all collected DriveLock log data files into a single ZIP file. If one of these files would have been manipulated to make use of the detected vulnerability, this would only cause the DriveLock Support Companion to crash.

A full list of related CVEs is available listed in the following section.

References

- NIST: <https://nvd.nist.gov/vuln/detail/CVE-2018-25032>

Mitigation

This vulnerability can be mitigated by not using the DriveLock Support Agent to collect all trace files or use the DOC to collect and upload the trace files.

How to update your environment

A patch for DriveLock 2022.1 and our latest long-term support release 2021.2 has been released. Customers can update their DriveLock agents to one of these two versions. We recommend to always use the latest available version.

3.2 Security Bulletin #22-002 - Log4net external library vulnerability

First published: **4th July 2022**

Last updated: **4th July 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of the Log4net library. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

DriveLock uses Log4Net to create log files for the client security awareness viewer component and the DES.

A full list of related CVEs is available listed in the following section.

References

- NIST: <https://nvd.nist.gov/vuln/detail/CVE-2018-1285>

Mitigation

This vulnerability can be mitigated by explicitly limit access to the XML configuration files (read only).

How to update your environment

Beginning with our next long-term support release 2022.2 DriveLock will use an updated version 2.0.14 for creating log files with Log4Net. Customers can update to this version as soon as it has been released.

3.3 Security Bulletin #22-003 - DotNetZip.Semvered external library vulnerability

First published: **4th July 2022**

Last updated: **4th July 2022**

Severity: **Low**

Summary

A vulnerability has been found in the implementation of DotNetZip.Semvered before 1.11.0. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

DotNetZip.Semvered before 1.11.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.

The DriveLock security awareness component and the DES use this component to unzip content, which was previously packed by DriveLock itself.

A full list of related CVEs is available listed in the following section.

References

- NIST: <https://nvd.nist.gov/vuln/detail/CVE-2018-1002205>

Mitigation

Beginning with our next release 2022.2 DriveLock will use a different library for handling ZIP files. Customers can then update to this version.

How to update your environment

All customers can update their environment as soon our new version DriveLock 2022.2 has been officially released.

3.4 Security Bulletin #22-004 - Node.js external library vulnerability

First published: **13th July 2022**

Last updated: **13th July 2022**

Severity: **None**

Summary

A vulnerability has been found in the implementation of Node.js. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- DriveLock 2020.2
- DriveLock 2021.1
- DriveLock 2021.2
- DriveLock 2022.1

Description

The detected vulnerabilities in Node.js allow execution of arbitrary code by a remote & anonymous attacker, which can be used to manipulate or circumvent security mechanisms.

The vulnerabilities **CVE-2022-32212**, CVE-2022-32213, CVE-2022-32214, CVE-2022-32215, CVE-2022-32222, **CVE-2022-32223** are collected in WID-SEC-2022-0621, the vulnerabilities with classification "High" are written in bold.

CVE-2022-32212: Only vulnerable via the command-line switch `node --inspect`, which enables the debugging interface of node and is not used by the DES server. It's not possible

to pass arbitrary arguments to the node runtime for a remote user, therefore this vulnerability cannot be exploited.

CVE-2022-32213, CVE-2022-32214, CVE-2022-32215: HTTP Request Smuggling is not possible because the node http api is behind a reverse proxy which does its own header parsing and validation.

CVE-2022-32222: Not applicable because it only affects Linux systems and the attacker would need local access to the DES.

CVE-2022-32223: The attacker needs local access to the DES server and needs write access to the DES service's user profile. Using the DES server alone, there is no way to exploit this remotely.

References

- BSI: <https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2022-0621>
- Node.js: <https://nodejs.org/en/blog/vulnerability/july-2022-security-releases/>

Mitigation

Drivelock cannot be targeted using these exploits.

How to update your environment

Customers do not need to update their environment.

Nevertheless we always recommend to use the latest available version.

3.5 Security Bulletin #22-005 - OpenSSL 3.0 external library vulnerability

First published: **4th November 2022**

Last updated: **4th November 2022**

Severity: **None**

Summary

Two vulnerabilities have been found in the implementation of OpenSSL. This affects the following supported DriveLock products (supported by the time this bulletin was created):

- No DriveLock product is affected

Description

The detected vulnerabilities (CVE-2022-3602 and CVE-2022-3786) in OpenSSL allow execution of arbitrary code using a buffer overrun which can be triggered in X.509 certificate verification, specifically in name constraint checking.

References

- OpenSSL: <https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/>
- NIST: <https://nvd.nist.gov/vuln/detail/CVE-2022-3602>
- NIST: <https://nvd.nist.gov/vuln/detail/CVE-2022-3786>

Mitigation

Drivelock cannot be targeted using these exploits.

How to update your environment

Customers do not need to update their environment.

Nevertheless we always recommend to use the latest available version.



Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2025 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

