Security Updates

In this category we inform you about the security updates contained in the current Shopware installation and update packages. You should install these immediately to keep your Shopware installation up-to-date and secure.

If you are not able to update your system to the latest version as recommended, you can use the Shopware Security Plugin to ensure that you have the latest security updates. The plugin closes current security gaps in your system, if it is activated in the backend. Please make sure to always update this plugin to the latest version.

Security Update 06/2023

Next to the usual bug fixes and optimisations, we have also been able to close vulnerabilities at the „low“ threat level.
Affected are the Shopware versions from 5.1.4 to 5.7.17
The following vulnerabilities, were fixed with this security update:

- SW-27070: Dependency configuration file exposed (since 5.6.0 CVE-2023-34098)
- SW-27102: Improper mail validation (since 5.1.4 CVE-2023-34099)

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.18. You can get the update to 5.7.18 regularly via the Auto-Updater or directly via the download overview.

Download Shopware

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 09/2022

Next to the usual bug fixes and optimisations, we have also been able to close vulnerabilities at the „low“ threat level.
Affected are the Shopware versions from 5.0.0 to 5.7.14
The following vulnerabilities, were fixed with this security update:

- SW-26909: Sensitive data in customer module (since 5.0.0 CVE-2022-36101)
- SW-26913: ACL could be bypassed (since 5.0.0 CVE-2022-36102)

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.15. You can get the update to 5.7.15 regularly via the Auto-Updater or directly via the download overview.

Download Shopware

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 07/2022

Next to the usual bug fixes and optimisations, we have also been able to close vulnerabilities at the „moderate“ threat level.

Affected are the Shopware versions from 5.7.0. to 5.7.13
The following vulnerabilities, were fixed with this security update:

- SW-26866: Persistent XSS (since 5.7.0 CVE-2022-31148)

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.14. You can get the update to 5.7.14 regularly via the Auto-Updater or directly via the download overview.

Download Shopware

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 06/2022

Next to the usual bug fixes and optimisations, we have also been able to close vulnerabilities at the „moderate“ threat level.
Affected are the Shopware versions from 5.0.0. to 5.7.11
The following vulnerabilities, were fixed with this security update:

- SW-26748: Persistent XSS (since 5.0.0 CVE-2022-31057)

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.12. You can get the update to 5.7.12 regularly via the Auto-Updater or directly via the download overview.

Download Shopware

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 04/2022

Next to the usual bug fixes and optimisations, we have also been able to close vulnerabilities at the „low“ threat level.
Affected are the Shopware versions from 5.0.0. to 5.7.8
The following vulnerabilities, were fixed with this security update:

- SW-26657: Not-persistent XSS (since 5.0.0 CVE-2022-24873)
- SW-26662: Malfunction of CSRF token validation (since 5.2.0 CVE-2022-24879)
- SW-26666: Multiple generation of tokens for the password reset function (since 5.0.4 CVE-2022-24892)

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.9. You can get the update to 5.7.9 regularly via the Auto-Updater or directly via the download overview.

Download Shopware
Note:
Customers with a current session will get a CSRF token error once after the update.

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 01/2022

General Information

In this security release, we have been able to close security gaps of the threat level "medium". Affected are the Shopware versions from 5.0.0 up to and including 5.7.6. The following vulnerability has been fixed with this security update:

SW-26435: Arbitrary redirect while using certain URLs (5.0.0 - 5.7.6)
SW-26448: Automatically invalidate sessions upon password change (5.7.3 - 5.7.6)

We recommend updating to the current version 5.7.7. You can get the update to 5.7.7 regularly via the Auto-Updater or directly via the download overview.

Download Shopware

This release reintroduces the automatic logout on password change. This function was not available in versions v5.7.3 - v5.7.6.
All customers with existing sessions will need to log in again after the update.

For older versions, corresponding security measures are also available via a plugin.

Shopware Security Plugin

Security update 10/2021

General information

In this security release, in addition to the usual bug fixes and optimizations, we have also been able to close security vulnerabilities of the threat levels "low" to "medium" in the frontend.

Affected are the Shopware versions from 5.0.0. to 5.7.5 The following vulnerabilities, were fixed with this security update:

- SW-26367 - Prevent authenticated stored XSS via SVG images

To secure your system, you can now choose between the following options:

Solutions

apache Webserver

If you are using **apache** as your web server, the **.htaccess**-file in the root directory of your Shopware installation should contain the following section:

```
<IfModule mod_headers.c>
    <FilesMatch "\.(?i:svg)$">
        Header set Content-Security-Policy "script-src 'none'"
    </FilesMatch>
</IfModule>
```

If this is not the case, please add the section manually or install / update the security plugin.

Install / update security plugin

- Download the Shopware security plugin version 1.1.25 from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

nginx Webserver

If you are using **nginx** as your web server, the configuration is not done using the **.htaccess** we provide. In this case, please add the following to your configuration file:

```
server {
    # ...
```

```
    location ~* ^.+\.svg$ {
        add_header Content-Security-Policy "script-src 'none'";
    }
}
```

Security Update 06/2021

General information

In this security release, in addition to the usual bug fixes and optimizations, we have also been able to close security vulnerabilities of the threat levels "low" to "medium" in the frontend.

Affected are the Shopware versions from 5.0.0. to 5.7.1 The following vulnerabilities, were fixed with this security update:

- SW-26108: Remote code execution in an external library

To secure your system, you can now choose between the following options:

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.7.2. You can get the update to 5.7.2 using the auto-updater or directly from our download overview.

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin version 1.1.23 from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 05/2021

General information

In this security release, in addition to the usual bug fixes and optimizations, we have also been able to close security vulnerabilities of the threat levels "low" to "medium" in the frontend.

Affected are the Shopware versions from 5.0.0. to 5.6.9 The following vulnerabilities, were fixed with this security update:

- SW-26001: SW-26001: Information leakage
- SW-26050: Authenticated Stored XSS in Shopware

To secure your system, you can now choose between the following options:

Solutions

Update the Shopware installation (Recommended)

We recommend updating to the current version 5.6.10. You can get the update to 5.6.10 using the auto-updater or directly from our download overview.

Install / update security plugin

If you can't update your Shopware installation (recommended), you can also secure it using a plugin:

- Download the Shopware security plugin version 1.1.22 from the store or alternatively directly from the plugin manager in the backend.
- Install and activate the plugin

If the plugin already exists, you can simply update the plugin through the plugin manager to bring it up to date. If problems occur, you can disable individual fixes using the plugin settings.

Please check all important functionalities after installation or update, especially the ordering process.

Security Update 11/2020

General information

Next to the usual bug fixes and optimisations, we have also been able to close multiple vulnerabilities at the „moderate“ threat level.

All Shopware Versions from 5.0.0 up to 5.6.8 are affected. The following vulnerabilities are fixed with this release.

- SW-25771: XSS in shopping worlds
- SW-25772: XSS in newsletter modules
- SW-25773: XSS in customer modules

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.6.9). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.21 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 06/2020

General information

Next to the usual bug fixes and optimisations, we have also been able to close a vulnerability at the „moderate“ threat level.
The Shopware Version 5.0.0 up to 5.6.6 are is affected. The following vulnerability is fixed with this release:

- SW-25409: Data of another client visible in the blog comment

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.6.7). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.20 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 10/2019

General information

Next to the usual bug fixes and optimisations, we have also been able to close a vulnerability at the „moderate“ threat level.
The Shopware Version 5.4.5 up to 5.6.1 are is affected. The following vulnerability is fixed with this release:

- SW-24590: Information Leakage

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.6.2). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.19 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 09/2019

General information

Next to the usual bug fixes and optimisations, we have also been able to close a vulnerability at the „moderate“ threat level.
The Shopware Version 5.6.0 is affected. The following vulnerability is fixed with this release:

- SW-24473: Not-persistent XSS

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.6.1). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.18 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 06/2019

General information

Next to the usual bug fixes and optimizations, we have also been able to close multiple vulnerabilities at the „moderate“ threat level.
All Shopware Versions from 5.1.0 up to 5.5.8 are affected. The following vulnerabilities are fixed with this release.

- SW-24068: Authenticated Remote Code Execution

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.5.9). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.17 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 04/2019

General information

Next to the usual bug fixes and optimisations, we have also been able to close multiple vulnerabilities at the „moderate“ threat level.
All Shopware Versions from 5.0.0 up to 5.5.7 are affected. The following vulnerabilities are fixed with this release.

- SW-23603: Not-persistent XSS
- SW-23626: Authenticated DQL injection
- SW-23766: SQL injection

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.5.8). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.15 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 02/2019

General information

Next to the usual bug fixes and optimisations, we have also been able to close multiple vulnerabilities at the „moderate“ threat level.
All Shopware Versions from 5.0.0 up to 5.5.6 are affected. The following vulnerabilities are fixed with this release.

- SW-23166, SW-23428: Session Fixation
- SW-23007: CSRF Token Leakage
- SW-23319: Non-persistent XSS

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.5.7). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.14 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 12/2018

General information

Next to the usual bug fixes and optimisations, we have also been able to close multiple vulnerabilities at the „moderate“ to „heavy“ threat level.
All Shopware Versions from 5.0.0 up to 5.5.3 are affected. The following vulnerabilities are fixed with this release.

- SW-23009, SW-23010: Authenticated remote code execution in the backend
- SW-23011: Path traversal with live media migration enabled
- SW-23012: Allows a Validation Bypass attack
- SW-23008: MITM vulnerability in update mechanism for incorrectly configured server systems

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.5.4). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.13 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 11/2018

General information

Next to the usual bug fixes and optimisations, we have also been able to close a vulnerability at the "medium" to "critical" threat level.
All Shopware Versions from 5.0.0 up to 5.5.2 are affected. The following vulnerabilities are fixed with this

release.

- SW-22811: Under certain conditions you could access cache files.

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware(5.5.3). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.12 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. If you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 10/2018

General information

Next to the usual bug fixes and optimisations, we have also been able to close multiple vulnerabilities at the "moderate to very low" threat level.
All Shopware Versions from 5.0.0 up to 5.5.1 are affected. The following vulnerabilities are fixed with this release.

- SW-22065: Allows XSS attack when CSRF protection is disabled.
- SW-22386: Authenticated backend or API user can execute malicious code via image upload

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.5.2). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin in version 1.1.11 from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. Also if you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 06/2018

General information

Next to the usual bug fixes and optimisations we have also been able to close a vulnerability at the "low" threat level. All Shopware Versions from 5.0.0 up to 5.4.3 are affected. The following vulnerabilities are fixed with this release.

- SW-21776: Authenticated Backend user with plugin installation permissions can upload unvalidated files via Plugin Manager

You can choose between two options to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware(5.4.4). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. Also if you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 05/2018

General information

Next to the usual bug fixes and optimizations, we have also been able to close multiple vulnerabilities at the "moderate to very low" threat level.
All Shopware Versions from 4.2.0 up to 5.4.2 are affected. The following vulnerabilities are fixed with this release.

- SW-21640: Information leakage
- SW-21593: Unauthorized currency change in ordering process
- SW-21404: Authenticated SQL Injection in the backend
- SW-21151: Authenticated path traversal attack in the REST API
- SW-21412: Authenticated path traversal attack in the backend

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.4.3). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment. Also if you experience any problems, you can disable individual fixes via the plugin settings.

Please check all important functionalities, in particular the ordering process, after installation or update

Security Update 02/2018

General information

Next to the usual bug fixes and optimisations, we have also been able to close two moderate vulnerabilities.
All Shopware Versions from 5.2.0 up to 5.3.7 are affected. The following vulnerabilities were fixed with this release.

- CSRF in the shopping cart
- CSRF in the checkout

You can choose between two options to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend you update to the latest version of Shopware (5.4.0). This version will fix these vulnerabilities. You can use the auto-update process or simply download the version on our download-page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security Plugin.

- Download the Shopware Security Plugin from our store or use the Plugin Manager in your Shopware backend.
- Install and activate the plugin.

If you already use this plugin, simply update it to the latest version to secure your environment.

After that, the option "Activate further protection of the checkout process against CSRF attacks" in the plugin settings should be activated to guarantee the necessary protection. Please check your system thoroughly after activation, since other plugins in use might cause unforeseen side effects.

Security Update 01/2018

General information

Next to the usual bug fixes and optimisations, we have also been able to close two moderate vulnerabilities.
All Shopware Versions from 5.2.0 up to 5.3.6 are affected. The following vulnerabilities are fixed with this release.

- SW-20878: Non-Persistent XSS in the Frontend (1)
- SW-20878: Non-Persistent XSS in the Frontend (2)

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.3.7). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment.

Security Update 10/2017

General information

Next to the usual bug fixes and optimisations, we have also been able to close three moderate vulnerabilities.
All Shopware Versions from 5.0.0 up to 5.3.3 are affected.

The following vulnerabilities are fixed with this release.

- SW-19834: Authenticated Backend and persistent XSS
- SW-19895: Authenticated Backend SQL Injection
- SW-19896: Authenticated Backend XXE

You can choose between two options, to protect your system:

Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware(5.3.4). This Version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download-page.

Install / update the security plugin

If it is not possible for you to update to the latest version of Shopware, you can use our Shopware Security-Plugin.

- Download the Shopware Security Plugin from our store or use the Plugin Manager of your Shopware backend.
- Install and activate the plugin.

If you use this plugin already, simply update it to the latest version to secure your environment.

Security Update 06/2017

General information

Under certain circumstances it is possible to execute an authorized foreign code in Shopware. This is a security vulnerability that could affect the entire system. All Shopware versions including Shopware 5.2.24

are affected. It is imperative that security updates be performed for every Shopware shop. Our current software version 5.2.25 already contains the required security update. You can upgrade to the new version 5.2.25 using the auto-update function in your backend or by downloading the release from our download page.

Alternate Solutions

Update Shopware (recommended)

We strongly recommend to update to the latest version of Shopware (5.2.25). This version will fix these vulnerabilities. You can use the auto-update process or simply download the version over our download page.

Patch plugin

- Download the following plugin: SwagSecurity
- Log into your Shopware backend and open the Plugin Manager
- Click on “Installed” (located on the left side of the window)
- Click on “Upload plugin” and select the plugin linked above
- Finally, install and activate the plugin within the overview in the Plugin Manager

This is a general security plugin. In the future potential security gaps can be fixed by updating this plugin. Although it is always recommended to update to the latest patchversion of Shopware.

Security Update 01/2017

Improved protection

Further information on the security update

Following the security update that was published on 23rd January, we are now providing you with an updated version that offers improved protection using only a few minor adjustments in Shopware. Under certain circumstances it is still possible to compromise Shopware and the HotFix plugin that was previously provided. One possible threat is if a template that doesn’t derive from the Shopware standard has been completely copied. To prevent this scenario, we created an updated version of Shopware (5.2.16) and the HotFix plugin (1.1.0). To ensure security, we strongly recommend that you install the latest version of Shopware (5.2.16) or the most recent version of the HotFix plugin. Please check whether you use themes or plugins that execute or overwrite the following template code. In this case, we recommend that you also make the following template adjustments in the derived template file.

Affected file: emotion.tpl

Path template file "Emotion template": templates / _default / frontend / forms / elements.tpl
Path template file "Responsive template": themes/Frontend/Bare/frontend/forms/elements.tpl

The complete line beginning with: {eval var=$sSupport.sFields[$sKey]... should be exchanged with the following:

```
{$sSupport.sFields[$sKey]|replace:'{literal}':''|replace:'{/literal}':''|replace:'%*%':"{s nam
```

(These adjustments have already been implemented in Shopware 5.2.15)

Theme and plugin developers

All theme and plugin developers are encouraged to encouraged to update their existing themes/plugins using the abovementioned code.

What should I do?

- Update Shopware to 5.2.16 or update the plugin.
- Check and adapt the code in the plugins, custom themes or templates

Important security update

General information about the security update

Under certain circumstances, it’s possible to execute an unauthorized foreign code in Shopware. This is a critical security vulnerability that could affect the entire system. All Shopware versions including Shopware 5.2.14 are affected. It is imperative that security updates be performed for every Shopware shop. Our current software version 5.2.15 already contains the required security update. You can upgrade to the new version 5.2.15 using the auto-update function in your backend or by downloading the release from our download page.

Alternatives for securing your system

If you are unable to upgrade your system to version 5.2.15 (recommended), you have another option for securing your system:

Patch plugin

- Download the following plugin: SwagSecurityHotFix201701
- Log into your Shopware backend and open the Plugin Manager
- Click on "*Installed*" (located on the left side of the window)
- Click on "*Upload plugin*" and select the plugin linked above
- Finally, install and activate the plugin within the overview in the Plugin Manager

Security Update 10/2016

General information

Under certain circumstances, it’s possible to execute an unauthorized foreign code in Shopware. This is a critical security vulnerability that could affect the entire system. All Shopware versions from 4.0.0 up to and including Shopware 5.2.8 are affected. It is imperative that security updates be performed for every Shopware shop. Our current software version 5.2.9 already contains the required security update. You can upgrade to the new version 5.2.9 using the auto-update function in your backend or by downloading the release from our download-page.

Alternatives for securing your system

If you are unable to upgrade your system to version 5.2.9 (recommended), you have two other options for securing your system:

Patch plugin

1. Download the following plugin: SwagSecurityHotFix201610.zip
2. Log into your Shopware backend and open the Plugin Manager
3. Click on “Installed” (located on the left side of the window)
4. Click on “Upload plugin” and select the plugin linked above
5. Finally, install and activate the plugin within the overview in the Plugin Manager

Manual fix

1. Download the following file: ManualHotFix201610.zip
2. Unzip the file in the main directory of your Shopware installation
3. Replace the existing engine/Shopware/Components/StringCompiler.php file

Security Update 04/2016

General information

Under certain conditions it is possible to execute unauthorized code in Shopware. This is a critical security vulnerability that not only affect the functions of the shop. It can also have an impact on the overall system. The vulnerability affects all Shopware versions 4.0.0 up to 5.1.4. Currently no cases are known in which the vulnerability has been actively exploited, but we strongly recommend to upgrade to the current version (5.1.5 or 4.3.7) of Shopware. If it is not possible to update to this versions of Shopware, please perform one of the following steps:

Alternate Solutions

Licence plugin version 1.1.2

When you use the license plugin version 1.1.2, you are not affected by the vulnerability. If you running an older version, it is highly recommend to update to 1.1.2.

Installing the patch plugins

1. Download the plugin SwagSecurityHotFix201604.zip
2. Log in to your shopware backend and open the Plugin Manager
3. Click on "installed"
4. Click on "Upload Plugin". Then select the just downloaded file and click "Upload Plugin"
5. Finally, activate the Patch Plugin