Security Updates

In this category we inform you about the security updates regarding Shopware 6. You should install these immediately to keep your Shopware installation up-to-date and secure.

Security Update 01/2024

General Information

In this security release, we have resolved a vulnerability of threat level "critical" to "moderate". Affected are all Shopware versions up to and including 6.5.7.3. The following issues have been fixed with this security update:

NEXT-32886 Server-Side Request Forgery (SSRF) in Flow Builder

NEXT-32887 Time-based blind SQL-injection Shopware CMS Search API

NEXT-32889 Broken Access Control order API

NEXT-33027 Vulnerability in composer package: dompdf/dompdf

We recommend updating to the current version 6.5.7.4. You can update to 6.5.7.4 via the auto-updater or manually via the download package.
https://www.shopware.com/en/download/#shopware-6

An update of the Commercial extension to 5.7.4 is also required for the NEXT-32886 vulnerability.

For older versions, corresponding security measures are also available via the central security plugin for Shopware 6. This includes the security measure, which is included in the Commercial extension update.

https://store.shopware.com/de/swag136939272659f/shopware-6-sicherheits-plugin.html

Security Update 07/2023

General Information

In this security release, we have resolved a vulnerability of the threat level "low". Affected are all Shopware

versions including 6.5.3.1. The following issue has been fixed with this security update:

NEXT-29146 - Composer league/oauth2-server upgrade, to fix a known security issue in that library.

The issue only exists if a non-standard key configuration is used in combination with an invalid key.
The key is also only exposed if exceptions are forwarded to the client. But it might be exposed in the logs regardless.

We recommend updating your 6.5 version to 6.5.3.2. You can update via the auto-updater.

For older versions you can check for one of these patterns in your configuration to figure out, if you are affected by this vulnerability:

shopware.yaml:

```
shopware:
    api:
        jwt_key:
            private_key_path: '%env(base64:JWT_PRIVATE_KEY)%'
            public_key_path: '%env(base64:JWT_PUBLIC_KEY)%'
```

or

services.yaml:

```
services:
    shopware.public_key:
        class: League\OAuth2\Server\CryptKey
        arguments: ["%env(base64:JWT_PUBLIC_KEY)%"]

    shopware.private_key:
        class: League\OAuth2\Server\CryptKey
        arguments: ["%env(base64:JWT_PRIVATE_KEY)%"]
```

Please get in touch with your agency, if you find these patterns in your configuration. Unfortunately, due to technical reasons, it is not possible for us to provide a general solution for older versions and you might need an individual adjustment for your environment.

Security Update 05/2023

General Information

In this security release, we have resolved a vulnerability of the threat level "low". Affected are all Shopware versions including 6.4.20.1. The following issue has been fixed with this security update:

NEXT-26426 - Updated nyholm/psr7 dependency to the latest version, to fix a known security issue in that library. The issue does not affect Shopware directly but might affect plugins.

We recommend updating your 6.4 version to 6.4.20.2 or 6.5.0.0. You can update via the auto-updater or manually via the download package.
https://www.shopware.com/en/download/#shopware-6

Security Update 04/2023

General Information

In this security release, we have resolved a vulnerability of threat level "critical". Affected are all Shopware versions up to and including 6.4.20.0. The following issues have been fixed with this security update:

NEXT-26140 - Improve Twig Security Extension to verify PHP Closures in Twig Templates (GHSA-7v2v-9rm4-7m8f)

We recommend updating to the current version 6.4.20.1. You can update to 6.4.20.1 via the auto-updater or manually via the download package.
https://www.shopware.com/en/download/#shopware-6

For older versions, corresponding security measures are also available via the central security plugin for Shopware 6.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 01/2023

General Information

In this security release, we have resolved vulnerabilities of the threat level "critical" and "medium". Affected are all Shopware versions including 6.4.18.0. The following issues have been fixed with this security update:

NEXT-24667 - Remote code execution via Twig template functions.
NEXT-24679 - Logging data can contain sensitive information of password reset mails.
NEXT-24677 - Administration session is not cleared after long inactivity.
NEXT-23325 - Possibility to bypass selling limits within the checkout process.
NEXT-22891 - Newsletter route does not consider double-opt-in settings.

We recommend updating to the current version 6.4.18.1. You can update to 6.4.18.1 via the auto-updater or manually via the download package.
https://www.shopware.com/en/download/#shopware-6

For older versions, corresponding security measures are also available via the central security plugin for Shopware 6.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 10/2022

General Information

In this security release, we have been able to close a security gap of the threat level "medium". Affected are the Shopware versions including 6.4.15.1. The following vulnerability has been fixed with this security update:

NEXT-23464: Bump twig dependency to 3.4.3 (https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33)

We recommend updating to the current version 6.4.15.2. You can get the update to 6.4.15.2 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

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

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Upgrade Infos

Extensions, which changed the block `utilities_icon` in the twig file `Storefront/Resources/views/storefront/utilities/icon.html.twig`, need to do the changes from the Upgrade.md.

Security Update 04/2022

General Information

In this security release, we have been able to close security gaps of the threat level "medium" and "low". Affected are the Shopware versions including 6.4.10.0. The following vulnerability has been fixed with this security update:

NEXT-21034: Prevent assignment of sales channel context to customer if permissions are set

NEXT-21077: Update DomPDF

NEXT-21078: Blind SSRF in Admin SDK

We recommend updating to the current version 6.4.10.1. You can get the update to 6.4.10.1 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

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

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 03/2022

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "critical". Affected are the Shopware versions including 6.4.8.1. The following vulnerability has been fixed with this security update:

NEXT-20305: Modify Customers, create Orders without App Permission
NEXT-20309: HTTP caching is marking private HTTP headers as public
NEXT-20235: Always false condition in Security Plugin

We recommend updating to the current version 6.4.8.2. You can get the update to 6.4.8.2 regularly via the Auto-Updater or directly via the download overview.
https://www.shopware.com/en/download/#shopware-6

For older versions, corresponding security measures are also available via a plugin.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 02/2022

General Information

In this security release, we have been able to close security gaps of the threat level low and medium. Affected are the Shopware versions including 6.4.8.0. The following vulnerability has been fixed with this security update:

NEXT-19820: User session is not logged out if the password is reset via password recovery
NEXT-19276: HTML injection possibility in voucher code form

We recommend updating to the current version 6.4.8.1. You can get the update to 6.4.8.1 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

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

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 11/2021

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "critical". Affected are the Shopware versions from 6.4.0.0 up to and including 6.4.6.0. The following vulnerability has been fixed with this security update:

NEXT-17527: Manipulation des Cache mit individuellem HTML oder JavaScript.
NEXT-18273: Timestamp missing for events. This might enable wrong connections with the app.

We recommend updating to the current version 6.4.6.1. You can get the update to 6.4.6.1 regularly via the Auto-Updater or directly via the download overview.
https://www.shopware.com/en/download/#shopware-6

For older versions, corresponding security measures are also available via a plugin.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 08/2021

General Information

In this security release, we have been able to close security gaps of the threat level "medium" and "critical". All listed issues were discovered in an internal penetration test. Affected are the Shopware versions from 6.1.0 up to and including 6.4.3.0. The following vulnerability has been fixed with this security update:

NEXT-15601: Manipulation of product reviews via API.
NEXT-15673: Authenticated server-side request forgery in file upload via URL.
NEXT-15677: Cross-Site Scripting via SVG media files.
NEXT-15675: Insecure direct object reference of log files of the Import/Export feature.
NEXT-15669: Command injection in mail agent settings.

We recommend updating to the current version 6.4.3.1. You can get the update to 6.4.3.1 regularly via the Auto-Updater or directly via the download overview.
https://www.shopware.com/en/download/#shopware-6

For older versions of 6.3 and lower, corresponding security measures are also available via a plugin.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 24/06/2021

General Information

In this security release, we have been able to close security gaps of the threat level "critical". Affected are the Shopware versions from 6.1.0 up to and including 6.4.1.1. The following vulnerability has been fixed with this security update:

NEXT-15858: Remote code execution in an external library

We recommend updating to the current version 6.4.1.2. You can get the update to 6.4.1.2 regularly via the Auto-Updater or directly via the download overview.
https://www.shopware.com/en/download/#shopware-6

For older versions of 6.3 and lower, corresponding security measures are also available via a plugin.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 06/2021

General Information

In this security release, we have been able to close security gaps of the threat level "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.4.1.0. The following vulnerability has been fixed with this security update:

NEXT-14744: Private files publicly accessible with an external cloud storage provider.
NEXT-14883: Privilege escalation of created integrations.
NEXT-15183: The API route for order cancellation does not check the customer scope.

We recommend updating to the current version 6.4.1.1. You can get the update to 6.4.1.1 regularly via the Auto-Updater or directly via the download overview.
https://www.shopware.com/en/download/#shopware-6

For older versions of 6.3 and lower, corresponding security measures are also available via a plugin.
https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Solutions

If you are using an external storage provider, you should run the new CLI command "**s3:set-visibility**" after the update, to fix possible accessibility issues.

For the correct configuration of your storage provider you should have a look into the following change:
https://github.com/shopware/docs/commit/cd9385be9bf5f618dff165eafe98eebb5a8a3efd

The usage of external storage provider is also documented here:
https://developer.shopware.com/docs/guides/hosting/infrastructure/filesystem

Security Update 04/2021

General Information

In this security release, we have fixed a critical vulnerability in addition to the usual bug fixes, as well as two other general security improvements. Affected are the Shopware versions from 6.1.0 up to and including 6.3.5.2. The following vulnerabilities have been fixed with this security update:

NEXT-14533 - After order payment process manipulatable
NEXT-14188 - Protect .env via .htaccess in shopware root!
NEXT-14278 - Persistent Cross-site Scripting Vulnerability
NEXT-14482 - Aggregations are not protected by ApiAware

To make use of the fixes made with NEXT-14188 & NEXT-14278 please make sure to update your server config accordingly.

Nginx:
https://developer.shopware.com/docs/resources/references/config-reference/server/nginx

Apache:
The update to 6.3.5.3 or the installation of the security plugin will update the htaccess. If you want to do this by your own, copy this file: https://github.com/shopware/production/blob/6.3/.htaccess

We recommend updating to the current version 6.3.5.3. You can get the update to 6.3.5.3 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 03/2021

General Information

In this security release, we have been able to close security gaps of the threat level "low" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.3.5.1. The following vulnerability has been fixed with this security update:

NEXT-13664: Potential Session Hijacking
NEXT-13896: Authenticated remote code execution using plugin manager without ACL permissions

We recommend to update to the current version 6.3.5.2. You can get the update to 6.3.5.2 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 02/2021

General Information

In this security release, we have fixed a critical vulnerability in addition to the usual bug fixes, as well as two other general security improvements. Affected are the Shopware versions from 6.1.0 up to and including 6.3.5.0. The following vulnerabilities have been fixed with this security update:

NEXT-13371 - Leak of information via Store-API
NEXT-12824 - Generation of fake documents via public GET-call
NEXT-13247 - Improvement of API token invalidation

The vulnerability from NEXT-13371 could only be fixed by changing the API system, which involves a non-backward-compatible change. Only consumers of the Store-API should be affected by this change. Please check your plugins if you have it in use. Detailed technical information can be found in the upgrade information.

We recommend to update to the current version 6.3.5.1. You can get the update to 6.3.5.1 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version.

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 12/2020

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.3.4.0. The following vulnerability has been fixed with this security update:

NEXT-12359: Information exposure via query strings in URL
NEXT-9689: Authenticated Server Side Request Forgery
NEXT-12230: Authenticated Privilege Escalation

We recommend to update to the current version 6.3.4.1. You can get the update to 6.3.4.1 regularly via the

Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. However, these do not include the full range of functions in the area of subsequent processing of orders that were created via a guest account, but only prevent misuse by deactivating the function. For the full range of functions, we recommend updating to the latest Shopware version.

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 10/2020

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.3.2.0. The following vulnerability has been fixed with this security update:

NEXT-10905: Authenticated XML External Entity Processing
NEXT-10909: Denial of Service via Cache Flooding

We recommend to update to the current version 6.3.2.1. You can get the update to 6.3.2.1 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2 the corresponding changes are also available via plugin:

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 09/2020

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.3.1.0. The following vulnerability has been fixed with this security update:

NEXT-10621 - RCE in third party library
NEXT-10624 - Non-persistent XSS in the Storefront

We recommend to update to the current version 6.3.1.1. You can get the update to 6.3.1.1 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 and 6.2 the corresponding changes are also available via plugin:

https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659

Security Update 07/2020

General Information

In this security release, we have been able to close security gaps of the threat level "low" and "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.2.2. The following vulnerability has been fixed with this security update:

NEXT-9176 - Authenticated stored XSS
NEXT-9175 - Authenticated Server Side Request Forgery
NEXT-9174 - Information Leakage when the development environment is active
NEXT-9240 - Authenticated stored XSS
NEXT-9569 - Session hijacking vulnerability of customer accounts in the storefront

We recommend to update to the current version 6.2.3. You can get the update to 6.2.3 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

For older versions of 6.1 the corresponding changes are also available via plugin:

Shopware 6 Security Plugin

Security Update 05/2020

General Information

In this security release, we have been able to close security gaps of the threat level "critical" and "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.1.5. The following vulnerability has been fixed with this security update:

NEXT-8571: Session hijacking vulnerability of customer accounts in the storefront.
NEXT-8282: Security update of third party symfony components.

We recommend to update to the current version 6.1.6. You can get the update to 6.1.6 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

Security Update 03/2020

General Information

In this security release, we have been able to close security gaps of the threat level "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.1.3. The following vulnerability has been fixed with this security update:

NEXT-7538: Product review user email exposed via sales channel API

We recommend to update to the current version 6.1.4. You can get the update to 6.1.4 regularly via the Auto-Updater or directly via the download overview.

https://www.shopware.com/en/download/#shopware-6

Security Update 02/2020

General Information

In this security release, we have been able to close security gaps of the threat level "medium" in addition to the usual error corrections and optimizations. Affected are the Shopware versions from 6.1.0 up to and including 6.1.1. The following vulnerability has been fixed with this security update:

NEXT-6618: Authenticated remote code execution via the administration

We recommend to update to the current version 6.1.2. You can get the update to 6.1.2 regularly via the Auto-Updater or directly via our download overview.

https://www.shopware.com/en/download/#shopware-6

Security Update 08/2019

General information

With the early access release 1.1 of shopware 6 we fixed a "critical" security vulnerability. The shopware developer preview and the early access version are affected.

NEXT-4341 - Validation bypass attack

Solution

You should update immediately to the newest version of shopware 6.

https://www.shopware.com/en/download/#shopware-6