Sicherheitsupdates

In dieser Kategorie informieren wir Dich über Sicherheitsupdates von Shopware 6. Diese solltest Du umgehend installieren, um Deine Shopware Installation aktuell und somit sicher zu halten.

Sicherheitsupdate 01/2024

Allgemeine Informationen

In diesem Update haben wir mehrere Sicherheitslücken der Bedrohungsstufe "kritisch" bis "moderat" beheben können. Betroffen sind alle Shopware Versionen bis einschließlich 6.5.7.3. Folgende Sicherheitslücken wurden mit diesem Update behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.5.7.4 durchzuführen. Das Update auf 6.5.7.4 kann direkt über den Auto-Updater oder manuell über das Download-Paket bezogen werden.
https://www.shopware.com/de/download/#shopware-6

Für die Sicherheitslücke NEXT-32886 ist darüber hinaus ein Update der Commercial Erweiterung auf 5.7.4 erforderlich.

Für ältere Versionen stehen entsprechende Sicherheitsmaßnamen ebenfalls über das allgemeine Sicherheits-Plugin zur Verfügung. Dies betrifft auch die Sicherheitsmaßnahme, die in der Commercial Erweiterung enthalten ist.

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

Sicherheitsupdate 07/2023

Allgemeine Informationen

In diesem Update haben wir eine Sicherheitslücke der Bedrohungsstufe "niedrig" beheben können. Betroffen sind alle Shopware Versionen bis einschließlich 6.5.3.1. Folgende Sicherheitslücke wurde mit diesem Update behoben:

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

Dieses Problem besteht nur, wenn eine nicht standardmäßige Key-Konfiguration in Kombination mit einem ungültigen Schlüssel verwendet wird.
Der Schlüssel ist nur sichtbar, wenn Exceptions an den Client weitergeleitet werden. Allerdings könnte es unabhängig davon auch in Logs einsehbar sein.

Wir empfehlen ein Update von 6.5.x auf die Version 6.5.3.2 durchzuführen. Das Update kann direkt über den Auto-Updater bezogen werden.

Für ältere Versionen können die Konfigurationsdateien auf folgende Muster überprüft werden, um herauszufinden, ob man von dieser Sicherheitslücke betroffen ist.

shopware.yaml:

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

oder

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)%"]
```

Bitte setze Dich mit deiner Agentur in Verbindung, wenn du diese Muster in deiner Konfiguration findest. Leider ist es für uns, aus technischen Gründen, nicht möglich eine allgemeine Lösung für Versionen älter als 6.5.0.0 anzubieten und es könnten individuelle Anpassungen für Deine Umgebung erforderlich sein.

Sicherheitsupdate 05/2023

Allgemeine Informationen

In diesem Update haben wir eine Sicherheitslücke der Bedrohungsstufe "niedrig" beheben können. Betroffen sind alle Shopware Versionen bis einschließlich 6.4.20.1. Folgende Sicherheitslücke wurde mit diesem Update behoben:

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.

Wir empfehlen ein Update auf die Version 6.4.20.2 oder 6.5.0.0 durchzuführen. Das Update auf

6.4.20.2 kann direkt über den Auto-Updater oder manuell über das Download-Paket bezogen werden.
https://www.shopware.com/de/download/#shopware-6

Sicherheitsupdate 04/2023

Allgemeine Informationen

In diesem Update haben wir eine Sicherheitslücke der Bedrohungsstufe "kritisch" beheben können. Betroffen sind alle Shopware Versionen bis einschließlich 6.4.20.0. Folgende Sicherheitslücken wurde mit diesem Update behoben:

NEXT-26140 - Twig Security Extension verbessert um PHP Closures zu überprüfen (GHSA-7v2v-9rm4-7m8f)

Wir empfehlen ein Update auf die aktuelle Version 6.4.20.1 durchzuführen. Das Update auf 6.4.20.1 kann direkt über den Auto-Updater oder manuell über das Download-Paket bezogen werden.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen stehen entsprechende Sicherheitsmaßnamen ebenfalls über das allgemeine Sicherheits-Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 01/2023

Allgemeine Informationen

In diesem Update haben wir Sicherheitslücken der Bedrohungsstufe "kritisch" und "mittel" beheben können. Betroffen sind alle Shopware Versionen bis einschließlich 6.4.18.0. Folgende Sicherheitslücken wurde mit diesem Update behoben:

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.

Wir empfehlen ein Update auf die aktuelle Version 6.4.18.1 durchzuführen. Das Update auf 6.4.18.1 kann direkt über den Auto-Updater oder manuell über das Download-Paket bezogen werden.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen stehen entsprechende Sicherheitsmaßnamen ebenfalls über das allgemeine Sicherheits-Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 10/2022

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir eine Sicherheitslücke der Bedrohungsstufe "mittel" schließen können. Betroffen sind die Shopware Versionen bis einschließlich 6.4.15.1. Folgende Sicherheitslücke wurde mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.4.15.2 durchzuführen. Das Update auf 6.4.15.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen stehen entsprechende Sicherheitsmaßnamen ebenfalls über eine Erweiterung zur Verfügung.

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

Upgrade Infos

Erweiterungen, die den Block `utilities_icon` in der Twig Datei `Storefront/Resources/views/storefront/utilities/icon.html.twig` angepasst haben, müssen die in der Upgrade.md hinterlegte Anpassung vornehmen.

Sicherheitsupdate 04/2022

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir Sicherheitslücken der Bedrohungsstufen "mittel" und "gering" schließen können. Betroffen sind die Shopware Versionen bis einschließlich 6.4.10.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.4.10.1 durchzuführen. Das Update auf 6.4.10.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen, stehen entsprechende Sicherheitsmaßnamen ebenfalls über eine Erweiterung zur Verfügung.

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

Sicherheitsupdate 03/2022

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir Sicherheitslücken der Bedrohungsstufen “kritisch” und “´gering” schließen können. Betroffen sind die Shopware Versionen bis einschließlich 6.4.8.1. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.4.8.2 durchzuführen. Das Update auf 6.4.8.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 02/2022

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir zwei Sicherheitslücken der Bedrohungsstufen “mittel” und “niedrig” schließen können. Betroffen sind die Shopware Versionen bis einschließlich 6.4.8.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.4.8.1 durchzuführen. Das Update auf 6.4.8.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung.

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

Sicherheitsupdate 11/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir Sicherheitslücken der Bedrohungsstufen "niedrig" und "kritisch" schließen können. Betroffen sind die Shopware Versionen von 6.4.0.0 bis einschließlich 6.4.6.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

NEXT-17527: Manipulation des Cache mit individuellem HTML oder JavaScript.
NEXT-18273: Fehlende Zeitstempel in App Events.

Wir empfehlen ein Update auf die aktuelle Version 6.4.6.1 durchzuführen. Das Update auf 6.4.6.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 08/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir Sicherheitslücken der Bedrohungsstufen "medium" und "kritisch" schließen können. Alle genannten Probleme wurden durch einen internen Penetration-Test erkannt. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.4.3.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

NEXT-15601: Produkt Bewertungen von anderen Benutzern konnten via API manipuliert werden.
NEXT-15671: Authentifizierte Server-Side Request Forgery beim Datei-Upload via URL.
NEXT-15677: Cross-Site Scripting in SVG Dateien.
NEXT-15675: Unsicherer Zugriff auf Log-Dateien im Import/Export Modul.
NEXT-15669: Unzureichende Zugriffsbeschränkung der Mailer-Konfiguration.

Wir empfehlen ein Update auf die aktuelle Version 6.4.3.1 durchzuführen. Das Update auf 6.4.3.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen der 6.3 und abwärts, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein

Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 24/06/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir eine Sicherheitslücke der Bedrohungsstufen „kritisch“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.4.1.1. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

NEXT-15858: Remote code execution in an external library

Wir empfehlen ein Update auf die aktuelle Version 6.4.1.2 durchzuführen. Das Update auf 6.4.1.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen der 6.3 und abwärts, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Sicherheitsupdate 06/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „medium“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.4.1.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

NEXT-14744: Private Dateien sind über externen Storage-Provider öffentlich zugänglich.
NEXT-14883: Erstellte Integrationen haben im Standard immer Admin-Rechte.
NEXT-15183: Die API Route für das Stornieren von Bestellungen berücksichtigt nicht den Kunden-Scope.

Wir empfehlen ein Update auf die aktuelle Version 6.4.1.1 durchzuführen. Das Update auf 6.4.1.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.
https://www.shopware.com/de/download/#shopware-6

Für ältere Versionen der 6.3 und abwärts, stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung.
https://store.shopware.com/detail/index/sArticle/518463/number/Swag136939272659

Lösungen

Solltest Du einen externen Storage-Provider im Einsatz haben, empfehlen wir den CLI-Befehl "**s3:set-visibility**" nach dem Update auszuführen, um mögliche Berechtigungsprobleme zu beheben.

Für eine korrekte Konfiguration Deiner externen Storage-Provider solltest Du folgende Einstellungsanpassung berücksichtigen:
https://github.com/shopware/docs/commit/cd9385be9bf5f618dff165eafe98eebb5a8a3efd

Die Verwendung von externen Storage-Providern ist hier dokumentiert:
https://developer.shopware.com/docs/guides/hosting/infrastructure/filesystem

Sicherheitsupdate 04/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen eine kritische Sicherheitslücke behoben, sowie zwei weitere Verbesserungen zur allgemeinen Sicherheit vorgenommen. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.5.2. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Um die mit NEXT-14188 & NEXT-14278 vorgenommenen Korrekturen zu nutzen, stellen Sie bitte sicher, dass Sie Ihre Serverkonfiguration entsprechend anzupassen.

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

Apache:
Mit dem Update auf 6.3.5.3 oder der Installation des Sicherheits-Plugins wird die htaccess aktualisiert. Um dies händisch vorzunehmen, kopiere diese Datei:
https://github.com/shopware/production/blob/6.3/.htaccess

Wir empfehlen ein Update auf die aktuelle Version 6.3.5.3. Sie können das Update auf 6.3.5.3 regelmäßig über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

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

Für ältere Versionen von 6.1 und 6.2 sind entsprechende Sicherheitsmaßnahmen auch über ein Plugin verfügbar. Für den vollen Funktionsumfang empfehlen wir ein Update auf die aktuelle Shopware-Version.

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

Sicherheitsupdate 03/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "leicht" schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.5.1. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.3.5.2 durchzuführen. Das Update auf 6.3.5.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 und 6.2 stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung. Für den vollen Funktionsumfang empfehlen wir das Update auf die neueste Shopware Version.

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

Sicherheitsupdate 02/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen eine kritische Sicherheitslücke behoben, sowie zwei weitere Verbesserungen zur allgemeinen Sicherheit vorgenommen. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.5.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Die Sicherheitslücke NEXT-13371 konnte nur durch eine Umstellung des API Systems behoben werden, was eine nicht abwärtskompatible Änderung beinhaltet. Es sollten nur Konsumenten der Store-API von dieser Änderung betroffen sein. Bitte überprüfe Deine Plugins, falls Du diese verwendets. Detaillierte technische Informationen findest Du in den Upgrade Informationen.

Wir empfehlen ein Update auf die aktuelle Version 6.3.5.1 durchzuführen. Das Update auf 6.3.5.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 und 6.2 stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung. Für den vollen Funktionsumfang empfehlen wir das Update auf die neueste Shopware Version.

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

Sicherheitsupdate 12/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "leicht" und „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.4.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.3.4.1 durchzuführen. Das Update auf 6.3.4.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 und 6.2 stehen entsprechende Sicherheitsmaßnamen ebenfalls über ein Plugin zur Verfügung. Diese beinhalten allerdings nicht den vollen Funktionsumfang im Bereich der nachträglichen Bearbeitung von Bestellungen, welche über ein Gastkonto erstellt wurden, sondern verhindern nur einen Missbrauch durch Deaktivierung der Funktion. Für den vollen Funktionsumfang empfehlen wir das Update auf die neueste Shopware Version.

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

Sicherheitsupdate 10/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "leicht" und „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.2.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.3.2.1 durchzuführen. Das Update auf 6.3.2.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 und 6.2 stehen die entsprechenden Änderungen ebenfalls über ein Plugin zur Verfügung:

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

Sicherheitsupdate 09/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "leicht" und „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.3.1.0. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.3.1.1 durchzuführen. Das Update auf 6.3.1.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 und 6.2 stehen die entsprechenden Änderungen ebenfalls über ein Plugin zur Verfügung:

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

Sicherheitsupdate 07/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "leicht" und „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.2.2. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

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

Wir empfehlen ein Update auf die aktuelle Version 6.2.3 durchzuführen. Das Update auf 6.2.3 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Für ältere Versionen der 6.1 stehen die entsprechenden Änderungen ebenfalls über ein Plugin zur Verfügung:

Shopware 6 Security Plugin

Sicherheitsupdate 05/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen "schwer" und „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.1.5. Folgende Sicherheitslücke, wurde mit diesem Sicherheitsupdate behoben:

NEXT-8571: Session Diebstahl von Benutzerkonten in der Storefront.
NEXT-8282: Security updates von Drittanbieter-Bibliotheken des Symfony frameworks.

Wir empfehlen ein Update auf die aktuelle Version 6.1.6 durchzuführen. Das Update auf 6.1.6 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Sicherheitsupdate 03/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.1.3. Folgende Sicherheitslücke, wurde mit diesem Sicherheitsupdate behoben:

NEXT-7538: Benutzer E-Mail von Produkt-Bewertungen ist über Sales-Channel API lesbar

Wir empfehlen ein Update auf die aktuelle Version 6.1.4 durchzuführen. Das Update auf 6.1.4 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Sicherheitsupdate 02/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „mittel“ schließen können. Betroffen sind die Shopware Versionen von 6.1.0 bis einschließlich 6.1.1 Folgende Sicherheitslücke, wurde mit diesem Sicherheitsupdate behoben:

NEXT-6618: Authentifizierte Remote Code Execution über die Administration

Wir empfehlen ein Update auf die aktuelle Version 6.1.2 durchzuführen. Das Update auf 6.1.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

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

Sicherheitsupdate 08/2019

Allgemeine Informationen

Mit dem Early Access Release 1.1 von Shopware 6 haben wir eine kritische Sicherheitslücke behoben. Es sind die Developer Preview und die Early Access Version betroffen.

NEXT-4341 - Validation bypass attack

Lösungen

Betroffene Systeme sollten so schnell wie möglich auf die neueste Version aktualisiert werden.

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