Sicherheitsupdates

In dieser Kategorie informieren wir Dich über die in den jeweils aktuellen Shopware Installations- und Updatepaketen enthaltenen Sicherheitsupdates. Diese solltest Du umgehend installieren, um Deine Shopware Installation aktuell und somit sicher zu halten.

Falls Du Dein System nicht, wie empfohlen, auf die neuste Version updaten kannst, sicherst Du Dich mit Updates des Shopware Sicherheits-Plugins ab. Das im Backend aktivierte Plugin schließt dann aktuelle Sicherheitslücken in Deinem System. Bitte achte darauf, dieses Plugin stets auf die aktuellste Version upzudaten.

Security Update 06/2023

Neben den üblichen Fehlerkorrekturen und Optimierungen, konnten wir auch Sicherheitslücken der Bedrohungsstufe "niedrig" schließen. Betroffen sind die Shopware-Versionen 5.1.4 bis 5.7.17
Die folgenden Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-27070: Dependency-Konfigurationsdatei auslesbar (seit 5.6.0 CVE-2023-34098)
- SW-27102: E-Mail Validierung in der Registration nicht hinreichend (seit 5.1.4 CVE-2023-34099)

Lösungen

Update der Shopware-Installation (empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.18. Du kannst das Update auf 5.7.18 regulär über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

Shopware herunterladen

Security-Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Security-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung

einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 09/2022

Neben den üblichen Fehlerkorrekturen und Optimierungen, konnten wir auch Sicherheitslücken der Bedrohungsstufe "niedrig" schließen. Betroffen sind die Shopware-Versionen 5.0.0. bis 5.7.14
Die folgenden Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-26909: Sensible Daten im Kundenmodul (seit 5.0.0 CVE-2022-36101)
- SW-26913: ACL kann umgangen werden (seit 5.0.0 CVE-2022-36102)

Lösungen

Update der Shopware-Installation (empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.15. Du kannst das Update auf 5.7.15 regulär über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

Shopware herunterladen

Security-Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Security-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 07/2022

Neben den üblichen Fehlerkorrekturen und Optimierungen, konnten wir auch Sicherheitslücken der Bedrohungsstufe "mittel" schließen. Betroffen sind die Shopware-Versionen 5.7.0. bis 5.7.13
Die folgenden Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-26866: Persistente XSS (seit 5.7.0 CVE-2022-31148)

Lösungen

Update der Shopware-Installation (empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.14. Du kannst das Update auf 5.7.14 regulär über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

Shopware herunterladen

Security-Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Security-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 06/2022

Neben den üblichen Fehlerkorrekturen und Optimierungen, konnten wir auch Sicherheitslücken der Bedrohungsstufe "mittel" schließen. Betroffen sind die Shopware-Versionen 5.0.0. bis 5.7.11
Die folgenden Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-26748: Persistente XSS (seit 5.0.0 CVE-2022-31057)

Lösungen

Update der Shopware-Installation (empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.12. Du kannst das Update auf 5.7.12 regulär über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

Shopware herunterladen

Security-Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Security-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 04/2022

Neben den üblichen Fehlerkorrekturen und Optimierungen, konnten wir auch Sicherheitslücken der Bedrohungsstufe "niedrig" schließen. Betroffen sind die Shopware-Versionen 5.0.0. bis 5.7.8
Die folgenden Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-26657: Nicht-persistente XSS (seit 5.0.0 CVE-2022-24873)
- SW-26662: Fehlfunktion der CSRF-Token-Validierung (seit 5.2.0 CVE-2022-24879)
- SW-26666: Mehrfache Erzeugung von Tokens für die Passwort-Zurücksetzen-Funktion (seit 5.0.4 CVE-2022-24892)

Lösungen

Update der Shopware-Installation (empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.9. Du kannst das Update auf 5.7.9 regulär über den Auto-Updater oder direkt über die Download-Übersicht beziehen.

Shopware herunterladen
Hinweis:
Kunden mit einer aktuellen Session werden einmalig nach dem Update einen CSRF-Token-Fehler bekommen.

Security-Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Security-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 01/2022

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir Sicherheitslücken der Bedrohungsstufe "medium" schließen können. Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.7.6. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

SW-26435: Willkürliche Weiterleitungen bei Benutzung von bestimmen URLs (5.0.0 - 5.7.6)
SW-26448: Automatische Invalidierung von Sessions beim Passwortwechsel (5.7.3 - 5.7.6)

Wir empfehlen ein Update auf die aktuelle Version 5.7.7 durchzuführen. Das Update auf 5.7.7 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Download Shopware

In diesem Release wurde der automatische Logout beim Passwortwechsel wieder eingeführt, diese Funktion war in den Versionen v5.7.3 - v5.7.6 nicht verfügbar.
Alle Kunden mit bestehenden Sessions werden sich hierdurch nach dem Update neu einloggen müssen.

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

Security Update 10/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ bis "mittel" im Frontend schließen können.
Betroffen sind die Shopware Versionen von 5.0.0. bis 5.7.5 Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-26367 - Authenticated stored XSS in SVG-Dateien verhindert

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

apache Webserver

Wenn Du **apache** als Webserver verwendest, sollte Deine **.htaccess**-Datei im Shopware-Stammverzeichnis folgende Sektion enthalten:

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

Ist das noch nicht der Fall, ergänze die Sektion bitte händisch, oder installiere / aktualisiere das Security-Plugin.

Security Plugin installieren / updaten

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.25 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

nginx Webserver

Wenn Du **nginx** als Webserver verwendest, erfolgt die Konfiguration nicht mittels der von uns gelieferten **.htaccess**.
Ergänze Deine Konfigurationsdatei in diesem Fall bitte wie folgt:

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

Security Update 06/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ bis "mittel" im Frontend schließen können.

Betroffen sind die Shopware Versionen von 5.0.0. bis 5.7.1 Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

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

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.7.2 durchzuführen. Das Update auf 5.7.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.23 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 5/2021

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ bis "mittel" im Frontend schließen können.

Betroffen sind die Shopware Versionen von 5.0.0. bis 5.6.9 Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

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

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.6.10 durchzuführen. Das Update auf 5.6.10 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du Deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.22 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins Besondere den Bestellprozess.

Security Update 11/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.6.8. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-25771: XSS in Einkaufswelten
- SW-25772: XSS in Newsletter Module
- SW-25773: XSS in Kunden Module

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.6.9 durchzuführen. Das Update auf 5.6.9 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.21 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 06/2020

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe „mittel“ schließen können.
Betroffen sind die Shopware Version 5.0.0 bis 5.6.6. Folgende Sicherheitslücke wurde mit diesem Sicherheitsupdate behoben:

- SW-25409: Daten eines anderen Kunden im Blog-Kommentar sichtbar

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.6.7 durchzuführen. Das Update auf 5.6.7 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.20 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten, ins besondere den Bestellprozess.

Security Update 10/2019

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe „mittel“ schließen können.
Betroffen sind die Shopware Version 5.4.5 bis 5.6.1. Folgende Sicherheitslücke wurde mit diesem

Sicherheitsupdate behoben:

- SW-24590: Unberechtigte Datenweitergabe

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.6.2 durchzuführen. Das Update auf 5.6.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.19 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten, ins besondere den Bestellprozess.

Security Update 09/2019

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe „mittel“ schließen können.
Betroffen ist die Shopware Version 5.6.0. Folgende Sicherheitslücke wurde mit diesem Sicherheitsupdate behoben:

- SW-24473: Nicht-persistente XSS

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.6.1 durchzuführen. Das Update auf 5.6.1 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.18 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten, ins besondere den Bestellprozess.

Security Update 06/2019

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ schließen können.
Betroffen sind die Shopware Versionen von 5.1.0 bis einschließlich 5.5.8. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-24068: Authentifizierte Remote Code Execution

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.9 durchzuführen. Das Update auf 5.5.9 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.17 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst Du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten, ins besondere den Bestellprozess.

Security Update 04/2019

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.5.7. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-23603: Nicht-persistente XSS
- SW-23626: Authentifizierte DQL Injection
- SW-23766: SQL-Injection

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.8 durchzuführen. Das Update auf 5.5.8 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.15 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 02/2019

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.5.6. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-23166, SW-23428: Session Fixation
- SW-23007: CSRF Token Leakage
- SW-23319: Nicht-persistente XSS

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.7 durchzuführen. Das Update auf 5.5.7 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.14 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 12/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch Sicherheitslücken der Bedrohungsstufen „gering“ bis „schwer“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.5.3. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-23009, SW-23010: Authentifizierte Remote Code Execution im Backend
- SW-23011: Path Traversal bei aktivierter Live-Medien-Migration
- SW-23012: Ermöglicht einen Validation Bypass Angriff
- SW-23008: MITM-Anfälligkeit in Updatemechanismus bei falsch konfigurierten Serversystemen

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.4 durchzuführen. Das Update auf 5.5.4 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.13 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.

- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 11/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe "mittel" bis "schwer" schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.5.2. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-22811: Unter bestimmten Bedingungen konnte man auf Cache-Dateien zugreifen

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen.

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.3 durchzuführen. Das Update auf 5.5.3 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.12 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 10/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe „gering“ und "mittel" schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.5.1. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-22065: Ermöglicht XSS Attacke, wenn CSRF-Schutz abgeschaltet ist.
- SW-22386: Authentifizierter Backend- oder API-Benutzer kann über den Bilderupload Schadcode ausführen

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.5.2 durchzuführen. Das Update auf 5.5.2 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin in Version 1.1.11 über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten insbesondere den Bestellprozess.

Security Update 06/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch eine Sicherheitslücke der Bedrohungsstufe „gering“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.4.3. Folgende Sicherheitslücken wurden mit diesem Sicherheitsupdate behoben:

- SW-21776: Authentifizierter Backend-Nutzer mit Plugin-Installationsrechten kann unvalidierte Dateien über Plugin-Manager hochladen

Um Dein System abzusichern kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.4.4 durchzuführen. Das Update auf 5.4.4 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten insbesondere den Bestellprozess.

Security Update 05/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch mehrere Sicherheitslücken der Bedrohungsstufe „moderat“ bis „sehr gering“ schließen können.

Betroffen sind die Shopware Versionen von 4.2.0 bis einschließlich 5.4.2. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-21640: Information Leakage
- SW-21593: Unerlaubte Währungsänderung im Bestellprozess
- SW-21404: Authentifizierte SQL Injection im Backend
- SW-21151: Authentifizierte Path Traversal Attacke in der REST API
- SW-21412: Authentifizierte Path Traversal Attacke im Backend

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.4.3 durchzuführen. Das Update auf 5.4.3 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen. Sollten Probleme auftreten, kannst du über die Plugineinstellung einzelne Fixes deaktivieren.

Überprüfe bitte nach Installation oder Update alle wichtigen Funktionalitäten ins besondere den Bestellprozess.

Security Update 02/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch zwei Sicherheitslücken der Bedrohungsstufe sehr gering bis gering schließen können.
Betroffen sind die Shopware Versionen von 5.2.0 bis einschließlich 5.3.7. Folgende

Sicherheitsschwachstellen, wurden mit diesem Sicherheitsupdate behoben:

- CSRF im Warenkorb
- CSRF im Checkout

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.4.0 durchzuführen. Das Update auf 5.4.0 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Seite.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager aktualisieren.

Anschließend sollte die Option "Activate further protection of the checkout process against CSRF attacks" in den Plugin Einstellungen aktiviert werden, damit der Schutz gewährleistet ist.

Bitte prüfe das System sorgfältig nach der Aktivierung, da es im Zusammenspiel mit den jeweils eingesetzten Plugins zu unerwartetem Verhalten führen kann.

Security Update 01/2018

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch zwei Sicherheitslücken der Bedrohungsstufe „moderat“ schließen können.
Betroffen sind die Shopware Versionen von 5.2.0 bis einschließlich 5.3.6. Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-20898: Nicht-persistente XSS im Frontend (1)

- SW-20898: Nicht-persistente XSS im Frontend (2)

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.3.7 durchzuführen. Das Update auf 5.3.7 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Seite.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen.

Security Update 10/2017

Allgemeine Informationen

In diesem Sicherheitsrelease haben wir neben den gewohnten Fehlerkorrekturen und Optimierungen auch drei Sicherheitslücken der Bedrohungsstufe „moderat“ schließen können.
Betroffen sind die Shopware Versionen von 5.0.0 bis einschließlich 5.3.3.

Folgende Sicherheitslücken, wurden mit diesem Sicherheitsupdate behoben:

- SW-19834: Authentifizierte persistente XSS im Backend
- SW-19895: Authentifizierte SQL Injection im Backend
- SW-19896: Authentifizierte XXE im Backend

Um Dein System abzusichern, kannst Du nun zwischen den folgenden Optionen wählen:

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.3.4 durchzuführen. Das Update auf 5.3.4 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

Falls Du deine Shopware-Installation nicht updaten kannst (empfohlen), kannst Du die Absicherung ebenso per Plugin vornehmen:

- Lade Dir das Shopware Sicherheits-Plugin über den Store herunter oder alternativ direkt über den Plugin-Manager im Backend.
- Installiere und aktiviere das Plugin

Falls das Plugin bereits vorhanden ist, kannst Du das Plugin einfach über den Plugin-Manager updaten, um es auf den neuesten Stand zu bringen.

Security Update 06/2017

Allgemeine Informationen

Unter bestimmten Voraussetzungen ist es derzeit möglich einen autorisierten Fremdcode in Shopware auszuführen. Dies ist eine Sicherheitslücke, die Auswirkungen auf das Gesamtsystem haben kann. Betroffen sind alle Shopware Versionen ab 4.0.0 bis einschließlich 5.2.24. Es ist daher zwingend erforderlich, das Sicherheitsupdate in jedem Shopware Shop einzuspielen. Unsere aktuell verfügbare Version 5.2.25 beinhaltet bereits das erforderliche Sicherheitsupdate. Das Update für 5.2.25 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Lösungen

Update der Shopware-Installation (Empfohlen)

Wir empfehlen ein Update auf die aktuelle Version 5.2.25 durchzuführen. Das Update auf 5.2.25 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Security Plugin installieren / updaten

- Lade Dir das Plugin SwagSecurity herunter
- Logge Dich in Dein Shopware Backend ein und öffne den Plugin Manager
- Klicke auf den Punkt "Installiert"
- Klicke auf "Plugin hochladen", wähle die gerade heruntergeladene Datei Plugin.zip aus und klicke auf "Plugin hochladen"

- Abschließend musst Du das Plugin im Plugin Manager aktivieren

Hierbei handelt es sich um ein generelles Sicherheitsplugin. Bei zukünftigen potenziellen Sicherheitslücken wird ein Update dieses Plugins bereitgestellt. Systeme, die kein Update (empfohlen) auf die aktuellste Patchversion von Shopware durchführen können, können über ein Update des Plugins abgesichert werden.

Security Update 01/2017

Allgemeine Informationen

Informationen zum Sicherheitsupdate

Für das am 23.01.2017 veröffentlichte Sicherheitsupdate stellen wir heute eine aktualisierte Version bereit, die über einen verbesserten Schutz auch bei individuellen Anpassungen von Shopware verfügt. Mit der ursprünglich bereitgestellten Lösung, Shopware 5.2.15 und dem HotFix-Plugin für ältere Versionen, ist es unter bestimmten Voraussetzungen möglich die Lücke weiterhin auszunutzen. Ein möglicher Angriffsvektor ist ein vollständig kopiertes Template, welches nicht sauber gemäß dem Shopware Standard abgeleitet worden ist. Damit auch dieses Szenario unterbunden werden kann, haben wir eine aktualisierte Version von Shopware und eine neue Version des HotFix-Plugins erstellt. Wir empfehlen die neueste Version von Shopware (5.2.16) oder die neue Version des HotFix Plugins (1.1.0) zu installieren. Überprüfe bitte zusätzlich, ob Du Themes oder Plugins einsetzt, die den folgenden Template Code ausführen oder überschreiben. Für diesen Fall empfehlen wir, an diesen Stellen die nachfolgenden Anpassungen in der abgeleiteten Template-Datei vorzunehmen.

Die betroffene Datei: elements.tpl.

Pfad Templatedatei Emotion Template: templates/_default/frontend/forms/elements.tpl
Pfad Templatedatei Responsive Template: themes/Frontend/Bare/frontend/forms/elements.tpl

Die komplette Zeile beginnend mit: {eval var=$sSupport.sFields[$sKey]... sollte mit dieser Zeile ausgetauscht werden:

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

(Diese Anpassung wurde bereits mit der Shopware Version 5.2.15 umgesetzt.)

Theme und Plugin Entwickler

Alle Theme und Plugin Entwickler sind angehalten die entsprechenden Zeilen in allen angebotenen Themes oder Plugins auszutauschen.

Was soll ich machen?

- Shopware Update auf 5.2.16 oder Aktualisierung des Plugins
- Prüfung & Anpassung der genannten Code-Stelle in Plugins / Custom Themes oder Templates

Wichtiges Sicherheitsupdate

Allgemeine Informationen zum Sicherheitsupdate

Unter bestimmten Voraussetzungen ist es möglich, einen unautorisierten Fremdcode in Shopware auszuführen. Dies ist eine kritische Sicherheitslücke, die Auswirkungen auf das Gesamtsystem haben kann. Betroffen sind alle Shopware Versionen ab 4.0.0 bis einschließlich 5.2.14. **Es ist zwingend erforderlich, das Sicherheitsupdate in jedem Shopware Shop einzuspielen.**Unsere aktuell verfügbare Version 5.2.15 beinhaltet bereits das erforderliche Sicherheitsupdate. Das Update für 5.2.15 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Übersicht.

Alternative Möglichkeiten zur Absicherung:

Sollte es Dir nicht möglich sein, das Update auf die Version 5.2.15 durchzuführen (empfohlen), gibt es eine weitere Möglichkeiten, Dein System abzusichern.

Patch-Plugin

- Lade Dir das Plugin SwagSecurityHotFix201701 herunter.
- Logge Dich in Dein Shopware Backend ein und öffne den Plugin Manager
- Klicke auf den Punkt "*Installiert*"
- Klicke auf "*Plugin Hochladen*". Danach wähle die gerade heruntergeladene Datei SwagSecurityHotFix201701.zip aus und klicke auf "*Plugin hochladen*"
- Abschließend musst Du das Plugin im Plugin Manager aktivieren.

Security Update 10/2016

Allgemeine Informationen

Unter bestimmten Voraussetzungen ist es möglich, einen unautorisierten Fremdcode in Shopware auszuführen. Dies ist eine kritische Sicherheitslücke, die Auswirkungen auf das Gesamtsystem haben kann. Betroffen sind alle Shopware Versionen ab 4.0.0 bis einschließlich 5.2.8. Es ist zwingend erforderlich, das Sicherheitsupdate in jedem Shopware Shop einzuspielen. Unsere aktuell verfügbare Version 5.2.9 beinhaltet bereits das erforderliche Sicherheitsupdate. Das Update für 5.2.9 kannst Du regulär über den Auto-Updater beziehen oder direkt über unsere Download-Seite.

Alternative Möglichkeit zur Absicherung

Sollte es Dir nicht möglich sein, das Update auf die Version 5.2.9 durchzuführen (empfohlen), gibt es zwei weitere Möglichkeiten Dein System abzusichern.

Patch-Plugin

1. Lade Dir das Plugin SwagSecurityHotFix201610.zip herunter.
2. Logge Dich in Dein Shopware Backend ein und öffne den Plugin Manager
3. Klicke auf den Punkt "Installiert"
4. Klicke auf "Plugin Hochladen". Danach wähle die gerade heruntergeladene Datei Plugin.zip aus und klicke auf "Plugin hochladen"
5. Abschließend musst Du das Plugin im Plugin Manager installieren und aktivieren.

Manueller Fix

1. Lade die Datei ManualHotFix201610.zip herunter.
2. Entpacke die Zipdatei in dem Hauptverzeichnis der Shopware-Installation
3. Ersetze die vorhandene engine/Shopware/Components/StringCompiler.php Datei

Security Update 04/2016

Allgemeine Informationen

Unter bestimmten Voraussetzungen ist es möglich, einen unautorisierten Fremdcode in Shopware auszuführen. Dieses ist eine kritische Sicherheitslücke, die Auswirkungen auf das Gesamtsystem haben kann. Betroffen sind alle Shopware Versionen ab 4.0.0 bis einschließlich 5.1.4. Aktuell sind uns keine Fälle bekannt in denen die Sicherheitslücke aktiv ausgenutzt wurde, jedoch ist es zwingend erforderlich, dass Sicherheitsupdate in jedem Shopware Shop einzuspielen. Unsere aktuell verfügbaren Versionen 5.1.5 und 4.3.7 beinhalten bereits das erforderliche Sicherheitsupdate.

Alternative Lösungen

Lizenzplugin 1.1.2

Wenn Du das Lizenzplugin in der Version 1.1.2 verwendest, bist Du nicht von der Lücke betroffen und entsprechend abgesichert. Solltest Du eine ältere Version besitzen, installiere bitte die aktuelle Version 1.1.2. über den Plug-In Manager.

Patch-Plugins

1. Lade das Plugin SwagSecurityHotFix201604.zip herunter.
2. Log Dich sich in Ihr Shopware Backend ein und öffne den Plugin Manager

3. Klicke auf den Punkt "Installiert"
4. Klicke auf "Plugin Hochladen". Danach wählst Du die gerade heruntergeladene Datei Plugin.zip aus und klickst auf "Plugin hochladen"
5. Abschließend musst Du das Plugin im Plugin Manager aktivieren.