Alerta de seguridad cibernética	9VSA20-00187-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2020
Última revisión	24 de abril de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por PrestaShop referente a vulnerabilidades que afectan al gestor de contenidos. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDADES

CVE-2020-5264
CVE-2020-5265
CVE-2020-5269
CVE-2020-5270
CVE-2020-5271
CVE-2020-5272
CVE-2020-5276
CVE-2020-5278
CVE-2020-5279
CVE-2020-5285
CVE-2020-5286
CVE-2020-5287
CVE-2020-5288
CVE-2020-5293

CVE-2020-5264

Debido a la falta de sanitización de datos ingresados por el usuario, un atacante podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.7.0.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-48vj-vvr6-jj4f
https://github.com/PrestaShop/PrestaShop/commit/06b7765c91c58e09ab4f8ddafbde02070fcb6f3a
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5264

CVE-2020-5265

Debido a la falta de sanitización de datos ingresados por el usuario en la página "AdminAttributesGroups", un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.7.6.1 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-7fmr-5vcc-329j
https://github.com/PrestaShop/PrestaShop/commit/622ba66ffdbf48b399875003e00bc34d8a3ef712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5265

CVE-2020-5269

Debido a la insuficiente sanitización de datos ingresados por el usuario entregados a través del parámetro “id_feature” en la página “AdminFeatures”, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.7.6.1 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-87jh-7xpg-6v93
https://github.com/PrestaShop/PrestaShop/commit/9efca621a0b74b82dafa91e6b955120036e31334
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5269

CVE-2020-5270

Debido a la insuficiente sanitización de datos entregados por el usuario a través del parámetro “back”, un atacante remoto podría crear un enlace que dirija hacia un sitio web confiable, pero que al entrar, redirija a un sitio arbitrario, permitiéndole realizar ataques phishing, robo de información sensible, conducir a la víctima a descarga de malware, etc.

Productos Afectados
PrestaShop desde la versión 1.7.6.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-375w-q56h-h7qc
https://github.com/PrestaShop/PrestaShop/commit/cd2219dca49965ae8421bb5a53fc301f3f23c458
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5270

CVE-2020-5271

Debido a la insuficiente sanitización de datos entregados por el usuario a través de los parámetros “date_from” y “date_to” en la página Dashboard, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.6.0.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-m2x6-c2c6-pjrx
https://github.com/PrestaShop/PrestaShop/commit/c464518d2aaf195007a1eb055fce64a9a027e00a
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5271

CVE-2020-5272

Debido a la insuficiente sanitización de datos entregados por el usuario a través de los parámetros “alias” y “search” en la página Search, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.5.5.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-rpg3-f23r-jmqv
https://github.com/PrestaShop/PrestaShop/commit/d3bf027fa37e8105fed3c809d636ebe787e43f46
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5272

CVE-2020-5276

Debido a la insuficiente sanitización de datos entregados por el usuario a través del parámetro "cartBox" en la página AdminCarts, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados

PrestaShop desde la versión 1.7.1.0 hacia adelante.

Mitigación

Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces

https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-q6pr-42v5-v97q
https://github.com/PrestaShop/PrestaShop/commit/6838d21850e7227fb8afbf568cb0386b3dedd3ef
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5276

CVE-2020-5278

Debido a la insuficiente sanitización de datos entregados por el usuario en la página Exception, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados

PrestaShop desde la versión 1.5.4.0 hacia adelante.

Mitigación

Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces

https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-mrpj-67mq-3fr5
https://github.com/PrestaShop/PrestaShop/commit/ea85210d6e5d81f058b55764bc4608cdb0b36c5d
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5278

CVE-2020-5279

Debido a inapropiadas restricciones de acceso a los controladores de legado y API, un atacante remoto y autenticado podría evadir ciertas medidas de seguridad y obtener acceso no autorizado a la aplicación.nack

- admin-dev/index.php/configure/shop/customer-preferences/
- admin-dev/index.php/improve/international/translations/
- admin-dev/index.php/improve/international/geolocation/
- admin-dev/index.php/improve/international/localization
- admin-dev/index.php/configure/advanced/performance
- admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses

Productos Afectados

PrestaShop desde la versión 1.5.0.0 hacia adelante.

Mitigación

Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces

https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-74vp-ww64-w2gm
https://github.com/PrestaShop/PrestaShop/commit/4444fb85761667a2206874a3112ccc77f657d76a
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5279

CVE-2020-5285

Debido a la insuficiente sanitización de datos entregados por el usuario a través del parámetro “back”, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados

PrestaShop desde la versión 1.7.6.0 hacia adelante.

Mitigación

Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces

https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-j3r6-33hf-m8wh
https://github.com/PrestaShop/PrestaShop/commit/b6aea152988d81e1586f1c03f2e72c9ef2fe7df7
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5285

CVE-2020-5286

Debido a la insuficiente sanitización de datos entregados por el usuario al subir un archivo equivocado, un atacante remoto podría enviarle a una víctima un enlace especialmente diseñado, para que al acceder ejecute el ataque XSS (Cross-site scripting) reflejado en el contexto del sitio vulnerable. Esto podría permitir al atacante robar credenciales, cambiar la apariencia del sitio, engañar a la víctima para que descargue malware, entre otras consecuencias.

Productos Afectados
PrestaShop desde la versión 1.7.4.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-98j8-hvjv-x47j
https://github.com/PrestaShop/PrestaShop/commit/fc0625fb0a9aab1835515f1bea52e8e063384da7
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5286

CVE-2020-5287

Debido a inapropiadas restricciones de acceso en la búsqueda “customers”, un atacante autenticado remoto podría evadir ciertas medidas de seguridad y obtener acceso no autorizado a la aplicación.

Productos Afectados
PrestaShop desde la versión 1.5.5.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-r6rp-6gv6-r9hq
https://github.com/PrestaShop/PrestaShop/commit/27e49d89808f1d76eb909a595f344a6739bc0b52
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5287

CVE-2020-5288

Debido a inapropiadas restricciones de acceso en la página “product attributes”, un atacante remoto y autenticado podría evadir ciertas medidas de seguridad y obtener acceso no autorizado a la aplicación.

Productos Afectados
PrestaShop desde la versión 1.7.0.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-4wxg-33h3-3w5r
https://github.com/PrestaShop/PrestaShop/commit/fc1d796dda769efdbc4d9e02ea7a11e4167338d0
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5288

CVE-2020-5293

Debido a inapropiadas restricciones de acceso en la página “product” con combinaciónes, adjuntos y precios especificos, un atacante remoto y autenticado podría evadir ciertas medidas de seguridad y obtener acceso no autorizado a la aplicación.

Productos Afectados
PrestaShop desde la versión 1.7.0.0 hacia adelante.

Mitigación
Actualizar a la versión 1.7.6.5 de PrestaShop.

Enlaces
https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-cvjj-grfv-f56w
https://github.com/PrestaShop/PrestaShop/commit/f9f442c87755908e23a6bcba8c443cdea1d78a7f
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5293