

Search	

Home Files News About Contact &[SERVICES\_TAB] Add New

Posted May 1, 2020

Follow us on Twitter

Subscribe to an RSS Feed

## xt:Commerce 5.4.1 / 6.2.1 / 6.2.2 Improper Access Control

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

xt:Commerce 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

Disclaimer:

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

Share This

LinkedIn

Reddit

Digg StumbleUpon

Su	Мо	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					

Top Authors In Last 30 Days	
Red Hat 154 files	
Ubuntu 73 files	
LiquidWorm 23 files	
Debian 18 files	
malvuln 11 files	
nu11secur1ty 11 files	
Gentoo 9 files	
Google Security Research 8 files	
T. Weber 4 files	
Julien Ahrens 4 files	

25 26 27 28 29 30

File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15,694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) CSRF (3,290) March 2022 DoS (22.602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2,899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14.201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30,044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12 469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

Download	LIKE IWAE
"Makes NO.512 NO	Change Mirror Download
Machinery Int STMS-7020-012 Froduct introduced to State of the State o	•
Froduct int Stockness Combail Mountering (150 1-16, 16, 21), 4, 21, Tested Version(5); 3-6, 16, 21, Version(7); 3-6,	Hash: SHA512
ValenceAbility Type: Improper Access Control (CMT-284) Halk Level: Bookland Manufacturer Notification: 2020-02-03 Solution Date: 2020-06-17 CMT Reference: CMT-2020-1201 Author of Andysolution CMT Reference: CMT-2020-1201 Author of Andysolution Marks Weller, Syd Comm  CMT Reference: CMT-2020-1201 Author of Andysolution CMT-2020-1201 Au	Product: xt:Commerce Manufacturer: xt:Commerce GmbH Affected Version(s): 5.4.1, 6.2.1, 6.2.2
Solution Date: 2020-04-01 Public Existories: 2020-04-01 Public Exi	Vulnerability Type: Improper Access Control (CWE-284) Risk Level: Medium Solution Status: Fixed
Markus Neiler, 9y56 Cobbi Tables Noros, 1 to switten in FNP and is available as both a free and paid version, xi:Commerce can also be extended via pluy-ins.  Due to improper access control, a logged-in user can clear other user addresses.  Valinerability 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 variet the data to. If the ID belongs to field in the address is set to null. An attacker could use this to null all addresses in a shop.  Proof of Concept (PoC):  Bending the following request with an existing address ID belonging to another customer nulls the fields for the inserted address ID:  POST /ds/customer/page_action-edit_address HTTP/l1[ []  action-edit_addressisaddress_book_id-[addressId]sold_address_class- defaultanddress_class-defaultscoutcomers_company-customers_gender—actioners_ifratnams-Postcoutcomers_gender—actioners_ifratnams-Postcoutcomers_dispensers_address  Solution:  Apply patch provided by the Banufacturer.  More information:  More information:  More information:  More information:  More information:  More information:  Ball the second of the second	Solution Date: 2020-04-17 Public Disclosure: 2020-04-30 CVE Reference: CVE-2020-12101
Overview:  XXI: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 PNP and is available plug-line.  Due to improper access control, a logged-in user can clear other user addresses.  Volumerability 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 the Address is a 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 null the fields for the inserted address ID:  Proof of Concept (PoC):  Sending the following request with an existing address ID belonging to another customer null the fields for the inserted address ID:  Proof of Concept (PoC):  Sending the following request with an existing address ID belonging to another customer null the fields for the inserted address ID:  Proof of Concept (PoC):  Sending the following request with an existing address INTEV.11  [11.  ***Existing Concept (PoC):  **Existing	Markus Weiler, SySS GmbH Fabian Krone, SySS GmbH
The product can be described as an online shop software which is mostly as both a free and paid version. It is suited in SUB and it a suitable 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.  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 IDB. On maving an address, an attacker could change the ID off the address to write the data to. If the ID belongs to field in the address is set to null. An attacker could use this to null all addresses in a shop.  Froof of Concept (PGC):  Sending the following request with an existing address ID belonging to another customer nulls the fields for the inserted address ID:  Froof /de/customer/page_action-edit_address MTTP/1.1  []  Froof /de/customer/page_action-edit_address/ATTP/1.1  []  action-edit_address_address_book_id-[address/ATTP/1.1]  []  Solution:  Solution:  Solution:  Solution:  Apply patch provided by the manufacturer.  More information:  https://hubydes.xt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch- 1704/2000-fr-xt-commerce-com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch- 1704/2000-fr-xt-commerce.com/ vulnerability during security assessment  2000-00-10: Extender reported found security vulnerability winerability to manufacturer  2000-00-10: Extender reported found security vulnerability winerability to manufacturer  2000-00-10: Extender reported found security vulnerability  Mttps://www.xys.de/fileadmin/dokumente/Publikationen/Advisories/XYSS-2020-012.txt  [3] SydS Responsible Disclosure Policy  https://www.ayss.de/fileadmin/dokumente/Publikationen/Advisories/XYSS-2020-012.txt  [3] SydS Responsible Disclosure Policy  https://www.ayss.de/fileadmin/dokumente/Publikationen/Advisories/XYSS-2020-012.txt  [4] Product w	
used in German speaking regions. It is written in PRP and is available as both a free and paid version, xticommerce can also be extended via plop-ins.  Due to improper access control, a logged-in user can clear other user addresses.  Vulnerability Details:  A logged-in customer and create and alter addresses. These addresses are Actes and alter addresses. These addresses are Actes and alter addresses. These addresses are Actes and alter addresses are Actes and alter addresses are Actes and a state and address and as 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:  Proof /de/customer/page_action-edit_address NTTP/l.1  []  FOST /de/customer/page_action-edit_address MTTP/l.1  []  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 MTTP/l.1  []  FOST /de/customer/page_action-edit_address MTTP/l.1  []  Sending the following request with an existing address class-defaultsaddress_class-defa	xt:Commerce is an online shop software.
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 variet he data to. If the ID belongs to the control of the address to variet he data to. If the ID belongs to the control of 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 HTTF/1.1 []  POST /de/customer?page_action=edit_address HTTF/1.1 []  POST /de/customer?page_action=edit_address HTTF/1.1 []  POST /de/customers_page_action=edit_address HTTF/1.1 []  POST /de/customers_page_action=edi	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
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 variet he data to. If the ID belongs to field in the address is set to write the data to. If the ID belongs to field in the address is set to nuil. An attacker could use this to nuil all addresses in a shop.  Proof of Concept (PoC):  Sending the following request with an existing address ID belonging to another customer nuils the fields for the inserted address ID:  POST /de/customer?page_action-edit_address HTPF/1.1  []  FOST /de/customer?page_action-edit_address HTPF/1.1  []  action-edit_address address book id-[addressId]sold_address_class-defaultCauddress_class-defaultCauddress_class-defaultCauddress_company=customers_gender=m6 customers_firstname=Pontcustomers_lastname=TestCcustomers_country_cod=DEA customers_personce=Usd3450789&customers_class-defaultCauddress_country_cod=DEA customers_phone=123450789&customers_first-customers_nountry_cod=DEA customers_first_cu	
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 variet he data to. If the ID belongs to field in the address is set to write the data to. If the ID belongs to field in the address is set to nuil. An attacker could use this to nuil all addresses in a shop.  Proof of Concept (PoC):  Sending the following request with an existing address ID belonging to another customer nuils the fields for the inserted address ID:  POST /de/customer?page_action-edit_address HTPF/1.1  []  FOST /de/customer?page_action-edit_address HTPF/1.1  []  action-edit_address address book id-[addressId]sold_address_class-defaultCauddress_class-defaultCauddress_class-defaultCauddress_company=customers_gender=m6 customers_firstname=Pontcustomers_lastname=TestCcustomers_country_cod=DEA customers_personce=Usd3450789&customers_class-defaultCauddress_country_cod=DEA customers_phone=123450789&customers_first-customers_nountry_cod=DEA customers_first_cu	
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 (PCC):  Sending the following request with an existing address ID belonging to smother 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-laddressId]&old_address_class= default&address class-default&customers_company-Gcustomers_gender=8 customers_firstname-Pen&customers_lastname-Test&customers_gender=8 customers_firstname-Pen&customers_lastname-Test&customers_obooker_code=8 customers_phone-123456789&customers_fax=&customers_street_address= Test&customers_postcode-123456789&customers_fax=&customers_street_address= Test&customers_postcode-123456789&customers_fax=&customers_street_address=8  PAPIN patch provided by the manufacturer.  Nors_information:  https://belpdas.wt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/addressbuch-sicherheitspatch-17042020-fr-xtcommerce.51-bis=622  Disclosure Timeline:  2020-01-23: Found security vulnerability during security assessment 2020-02-03: Scutomer reported found security vulnerability to sanufacturer 2020-03-03: Acknowledgement of security vulnerability to manufacturer 2020-03-03: Acknowledgement of security vulnerability  References:    Product website for xt.Commerce	
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 NTTP/1.1 []  POST /de/customer?page_action-edit_address NTTP/1.1 []  action-edit_address_class-defaultcoustomers_company=customers_gender=m6 customers_firstname=Penciousomers_lastname=Testcustomers_street_address=	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
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 NTTP/1.1 []  POST /de/customer?page_action-edit_address NTTP/1.1 []  action-edit_address_class-defaultcoustomers_company=customers_gender=m6 customers_firstname=Penciousomers_lastname=Testcustomers_street_address=	
another customer nulls the fields for the inserted address ID:  POST /de/customer?page_action=edit_address HTTP/1.1 []  post /de/customer?page_action=edit_address HTTP/1.1 []  action=edit_address_daddress_book_id=[addressId]&old_address_class= defaultkaddress_class=defaultcustomers_company=customers_gender=m6 customers_firstname=Penctousomers_latentame=Testcustomers_atreet_address= TestScustomers_postcode=12345:customers_clty=TestCustomers_customers_daddress= TestScustomers_postcode=12345:customers_clty=TestCustomers_custome	
action=edit_address_daddress_book_id=[addressId]sold_address_class= defaultsdadress_class=defaultscustomers_company=kcustomers_gender=ms_ customers_firstname=Penscustomers_lastname=Testscustomers_atreet_address= Testscustomers_postcode=1234867894customers_clavf=customers_company=kcustomers_company	
defaultsaddress_class-defaultcoutomers_company-koustomers_dender=ms customers_firstname=Pendcoutomers_latendame=Testcoutomers_street_address= TestGustomers_postcode=12345kcustomers_clty=TestCustomers_country_code=DEs customers_postcode=12345kcustomers_clty=TestCustomers_country_code=DEs customers_pone=12345f998customers_fax=Kustomers_country_code=DEs customers_pone=12345f998customers_fax=Kustomers_country_code=DEs customers_pone=12345f998customers_fax=Kustomers_country_code=DEs customers_country_code=DEs customers_country_code=DEs customers_country_country_code=DEs customers_country_country_country_code=DEs customers_country_country_country_country_country_code=DEs customers_country_co	
Apply patch provided by the manufacturer.  More information: https://helpdesk.xt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch- 1704/200-fr-crocommerce-51-bls-622  Disclosure Timeline:  2020-01-23; Found security vulnerability during security samesment 2020-03: Customer reported found security wulnerability to manufacturer 2020-03-10; Execurity advisory with further details sent to manufacturer 2020-03-11; Acknowledgement of security advisory by manufacturer 2020-04-17; Patch released by manufacturer 2020-04-17; Patch released by manufacturer 2020-04-17; Patch released by manufacturer 2020-04-10; Public disclosure of vulnerability  References:  [1] Product website for xt:Commerce     https://www.xt-commerce.com/ [2] SysS security advisory 938-2020-012  https://www.xys.de/fileadmin/dokumente/publimationen/Advisories/SYS-2020-012.txt [3] SysS seponshibe Disclosure Policy  https://www.ayss.de/en/news/responsible-disclosure-policy/  Credits:  E-Mail: markus.weiler@syss.de Public Key:     https://www.ayss.de/fileadmin/dokumente/PGPReys/Markus_Weiler.asc     key Dio OKCESMANDOSIOZBS  Rey Jingeptinit B958 4048 SPP3 885 F248 887A CEE9 4AZD 0510 2D89	default&address_class=default&customers_company=&customers_gender=m& customers_firstname=Pen&customers_lastname=Pest&customers_street_address= Test&customers_postcode=1234\$&customers_city=Test&customers_country_code=DE&
More information: https://helpdesk.xt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch- 17042020-ft-xtcommerce-Si-bis-622  Disclosure Timeline: 2020-01-23: Found security vulnerability during security assessment 2020-03: Customer reported found security vulnerability to manufacturer 2020-03-13: Security advisory with further details sent to manufacturer 2020-04-30: Fatch 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 978S-2020-012  https://www.yss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Policy     https://www.ayss.de/shiwaw/responsible-disclosure-policy/  Credits:  Credits:  E-Mail: markus.weiler@syss.de Public Key:     https://www.yss.de/fileadmin/dokumente/PGPReys/Markus Weiler.asc     key ID. OKCESWAN2D0510289 Rey Jingeptin: B9SS 4048 SPPO 389C F248 B87A CEE9 4A2D 0510 2D89	Solution:
https://www.yss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Formure June Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Formure June Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Found by Markus Weiler and Fabian Krone of SySS Genbil Warkus Weiler BySS Genbil Warkus Weiler and Fabian Krone of SySS Genbil Warkus Weiler BySS Genbil BySS Genbil Warkus Weiler BySS Genbil ByS	Apply patch provided by the manufacturer.
2020-01-23: Found security vulnerability during security assessment 2020-03: Customer reported found security vulnerability to sanufacturer 2020-03-10: Acknowledgement of security advisory by manufacturer 2020-03-11: Acknowledgement of security advisory by manufacturer 2020-04-17: Patch released by manufacturer 2020-04-19: Public disclosure of vulnerability  References:  [1] Product website for xt:Commerce     https://www.xt-commerce.com/ [2] Sy35 Security Advisory 3028-0020-012  https://www.xys.de/fileadmin/dokumente/fublikationen/Advisories/SYSS-2020-012.txt [3] Sy35 Responsible Disclosure Policy     https://www.sys.de/en/news/responsible-disclosure-policy/  Credits:  This security vulnerability was found by Markus Weiler and Fabian Krone of Sy35 Gabble.  E-Mail: markus.weiler@sys.de Public Key:     https://www.sys.de/fileadmin/dokumente/FGFKeys/Markus_Weiler.asc     key Ileagesh/2005102Ds9 Rey Ileagesh/2005102Ds9 Rey Ileagesh/2005102Ds9	https://helpdesk.xt-commerce.com/index.php?/Knowledgebase/Article/View/1784/294/adressbuch-sicherheitspatch-
2020-01-23: Found security vulnerability during security assessment 2020-03: Customer reported found security vulnerability to sanufacturer 2020-03-10: Acknowledgement of security advisory by manufacturer 2020-03-11: Acknowledgement of security advisory by manufacturer 2020-04-17: Patch released by manufacturer 2020-04-19: Public disclosure of vulnerability  References:  [1] Product website for xt:Commerce     https://www.xt-commerce.com/ [2] Sy35 Security Advisory 3028-0020-012  https://www.xys.de/fileadmin/dokumente/fublikationen/Advisories/SYSS-2020-012.txt [3] Sy35 Responsible Disclosure Policy     https://www.sys.de/en/news/responsible-disclosure-policy/  Credits:  This security vulnerability was found by Markus Weiler and Fabian Krone of Sy35 Gabble.  E-Mail: markus.weiler@sys.de Public Key:     https://www.sys.de/fileadmin/dokumente/FGFKeys/Markus_Weiler.asc     key Ileagesh/2005102Ds9 Rey Ileagesh/2005102Ds9 Rey Ileagesh/2005102Ds9	National Market
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 [3] SySS Responsible Disclosure Policy https://www.yss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Policy https://www.yss.de/en/news/responsible-disclosure-policy/  Credits:  This security vulnerability was found by Markus Weiler and Fabian Krone of SySS GabH.  B-Mail: markus.weiler@syss.de Public Key: https://www.yss.de/fileadmin/dokumente/PGFKeys/Markus_Weiler.asc https://www.asc	2020-01-23: Found security vulnerability during security assessment
[1] Product website for xt:Commerce https://www.xt-commerce.com/ [2] SySS Generity Advisory SYSS-2020-012 https://www.syss.de/fileadmin/dokumente/Sublikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Policy/ https://www.syss.de/en/news/responsible-disclosure-policy/  Credits:  Credits:  Credits:  E-Mail: markus.weiler@syss.de Public Key: https://www.syss.de/fileadmin/dokumente/FGFReys/Markus_Weiler.asc Rey LDD OKCED#AALDOS102BB9 Rey Independent: B9SS 4048 SDF0 389C F24B 8B7A CEEP 4AZD 0510 2DB9	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
[1] Product website for xt:Commerce https://www.xt-commerce.com/ [2] SySS Generity Advisory SYSS-2020-012 https://www.syss.de/fileadmin/dokumente/Sublikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Policy/ https://www.syss.de/en/news/responsible-disclosure-policy/  Credits:  Credits:  Credits:  E-Mail: markus.weiler@syss.de Public Key: https://www.syss.de/fileadmin/dokumente/FGFReys/Markus_Weiler.asc Rey LDD OKCED#AALDOS102BB9 Rey Independent: B9SS 4048 SDF0 389C F24B 8B7A CEEP 4AZD 0510 2DB9	References:
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.  F-Mail: markus.weiler@syss.de Public Rey; https://www.syss.de/fileadmin/dokumente/PGFKeys/Markus_Weiler.asc Key ID: 0xcERP420205102DB9 Key Fingerprint: B95E 4C48 50F0 389C F24B 8B7A CEE9 4A2D 0510 2DB9	[1] Product website for xt:Commerce https://www.xt-commerce.com/
Credits:  This security vulnerability was found by Markus Weiler and Fabian Krone of SySS (GBH).  FaMedi: markus.weiler8syss.de  Public Key:  https://www.syss.de/fileadmin/dokumente/PGPKeys/Markus_Weiler.asc  Key ID: OxCER042005102DB9  Key Fingerprint: B95E 4C48 50F0 389C F24B 8B7A CEE9 4AZD 0510 2DB9	https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt [3] SySS Responsible Disclosure Policy
This security vulnerability was found by Markus Weiler and Fabian Krone of SySS (GabH.  E-Mail: markus.weiler@syss.de Public Key: 1016 (Acceptable 1016) (Ac	https://www.syss.de/en/news/responsible-disclosure-policy/
of SySS GmbH.  E-Mail: markus.weiler@syss.de Public Keyr Https://www.yss.de/fileadmin/dokumente/PGFKeys/Markus_Weiler.esc Mcgr. docmEd942005102788 Mey 10 00CED4942005102788  ESP Fingespint: B95E 4C48 50F0 389C F248 887A CEE9 4AZD 0510 2D89	Credits:
Public Key: https://www.syss.de/fileadmin/dokumente/PGFKeys/Markus_Weiler.asc Key ID: OxCEE94AZDO5102DB9 Key Fingerprint: B95E 4C48 50F0 389C F24B 8B7A CEE9 4AZD 0510 2DB9	of SySS
Key ID: 0xCEE94A2D05102D89  Key Fingerprint: B95E 4C48 50F0 389C F24B 8B7A CEE9 4A2D 0510 2DB9	Public Key:
	Key ID: 0xCEE94A2D05102DB9
E-Mail: fabian.krone8yss.de Public Rey: https://www.syss.de/fileadmin/dokumente/PGFKeys/Fabian_Krone.asc Rey ID: OxBFDF30ABD10EADF4 Rey Finegerpint: OADE D2AA AEZ7 7DDA A8F0 C051 BFDF 30AB D10E A0F4	Key ID: 0xBFDF30ABD10EA0F4

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. Spoof (2,166) SUSE (1,444) SQL Injection (16,102) Ubuntu (8,199) TCP (2,379) UNIX (9,159) Copyright: UnixWare (185) Creative Commons - Attribution (by) - Version 3.0 URL: http://creativecommons.org/licenses/by/3.0/deed.en UDP (876) Windows (6,511) Virus (662) Other ----BEGIN PGP SIGNATURE-----IC BABELOLN PEW SIGNATURE——

OPTAHO/+PMURDOES-COTYCHNIA-FUTTGHNY-Ex/Lainfeld-SALCykOy-8wy92D

OPTAHO/+PMURDOES-COTYCHNIA-FUTTGHNY-Ex/Lainfeld-SALCykOy-8wy92D

OPTAHO/+PMURDOES-COTYCHNIA-FUTTGHNY-Ex/Lainfeld-SALCykOy-8wy92D

Syd2 Nex 1-y-1 Lhouknia-SALCykOy-8wy92D

Syd2 Nex 1-y-1 Lho Vulnerability (31,136) Web (9,365) Whitepaper (3,729) x86 (946) XSS (17,494) Other

## Login or Register to add favorites



## Site Links About Us News by Month History & Purpor

News Tags

History & Purpose

Contact Information

Files by Month Terms of Service
File Tags Privacy Statement
File Directory Copyright Information

## Hosting By Rokasec



