



CVE-2020-12101

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-12101
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-30 14:15:00 UTC
Updated	2020-05-06 18:32:00 UTC
Description	The address-management feature in xt:Commerce 5.1 to 6.2.2 allows remote authenticated users to zero out other user's s

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xt-commerce	Xt	commerce	All	All	All

References

Reference	Source	Link
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-012.txt	MISC	www.syss.de
Full Disclosure: [SYSS-2020-012] Improper Access Control (CWE-284) in xt:Commerce (CVE-2020-12101)	FULLDISC	seclists.org
Adressbuch Sicherheitspatch 17.04.2020 für xt:Commerce 5.1 bis 6.2.2 - Powered by Kayako Help Desk Software	CONFIRM	helpdesk.xt-commerce.com
xt:Commerce 5.4.1 / 6.2.1 / 6.2.2 Improper Access Control ≈ Packet Storm	MISC	packetstormsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report