



CVE-2011-5011

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

Summary

CVE	CVE-2011-5011
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-12-25 01:55:00 UTC
Updated	2017-08-29 01:30:00 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in xt:Commerce 3.0.4 SP2.1 and possibly earlier allow remote att

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xt-commerce	Xt	commerce	3.0.4	sp2.1	All
Application	Xt-commerce	Xt	commerce	3.0.4	sp2.1	All
Application	Xt-commerce	Xt	commerce	3.0.4	sp2.1	All

References

Reference	Source
index of /home/dishix/: xt:Commerce v3.0.4 SP2.1 Cross Site Request Forgery (CSRF) SECURITY ADVISORY - DISHIX 201111-01	MISC
index of /home/dishix/: Exploiting xt:Commerce v3.04 SP2.1 Cross Site Request Forgery (CSRF)	MISC
IBM X-Force Exchange	XF
About Secunia Research Flexera	SECU
77498	OSVD
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)