



CVE-2014-2230

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

Summary

CVE	CVE-2014-2230
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-23 14:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	Open redirect vulnerability in the header function in addclick.php in OpenX 2.8.10 and earlier allows remote attackers to redi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openx	Openx	2.8	All	All	All
Application	Openx	Openx	2.8.1	All	All	All
Application	Openx	Openx	2.8.2	All	All	All
Application	Openx	Openx	2.8.3	All	All	All
Application	Openx	Openx	2.8.4	All	All	All
Application	Openx	Openx	2.8.5	All	All	All
Application	Openx	Openx	2.8.6	All	All	All
Application	Openx	Openx	2.8.7	All	All	All
Application	Openx	Openx	2.8.8	All	All	All
Application	Openx	Openx	2.8.9	All	All	All
Application	Openx	Openx	2.8	All	All	All
Application	Openx	Openx	2.8.1	All	All	All
Application	Openx	Openx	2.8.2	All	All	All
Application	Openx	Openx	2.8.3	All	All	All
Application	Openx	Openx	2.8.4	All	All	All
Application	Openx	Openx	2.8.5	All	All	All
Application	Openx	Openx	2.8.6	All	All	All

Application	Openx	Openx	2.8.7	All	All	All
Application	Openx	Openx	2.8.8	All	All	All
Application	Openx	Openx	2.8.9	All	All	All
Application	Openx	Openx	All	All	All	All

References			
Reference	Source	Link	Tags
Full Disclosure: CVE-2014-2230 - OpenX Open Redirect Vulnerability	FULLDISC	seclists.org	Exploit
CVE-2014-2230 – OpenX Dest Redirect Privilege Escalation Vulnerability	MISC	www.tetrapph.com	Exploit
OpenX 2.8.10 Open Redirect ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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