



CVE-2018-14020

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

Summary

CVE	CVE-2018-14020
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-20 22:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in the Paymorrow module 1.0.0 before 1.0.2 and 2.0.0 before 2.0.1 for OXID eShop. An attacker c

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paymorrow	Paymorrow	1.0.0	All	All	All
Application	Paymorrow	Paymorrow	1.0.2	rc1	All	All
Application	Paymorrow	Paymorrow	2.0.0	All	All	All
Application	Paymorrow	Paymorrow	1.0.0	All	All	All
Application	Paymorrow	Paymorrow	1.0.2	rc1	All	All
Application	Paymorrow	Paymorrow	2.0.0	All	All	All

References

Reference	Source	Link
Security Bulletin 2018-003 • OXIDforge	CONFIRM	oxid
0006801: It is possible to bypass the check for delivery address changes during checkout process - OXID eShop bugtrack	CONFIRM	bug
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)