



CVE-2020-8818

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

Summary

CVE	CVE-2020-8818
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-25 02:15:00 UTC
Updated	2020-03-05 18:06:00 UTC
Description	An issue was discovered in the CardGate Payments plugin through 2.0.30 for Magento 2. Lack of origin authentication in th

Risk And Classification

Problem Types: CWE-346

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Magento	2.3.4	All	All	All
Application	Adobe	Magento	2.3.4	All	All	All
Application	Cardgate	Cardgate Payments	All	All	All	All

References

Reference

- [magento2/Callback.php at 715979e54e1a335d78a8c5586f9e9987c3bf94fd · cardgate/magento2 · GitHub](#)
- [Magento WooCommerce CardGate Payment Gateway 2.0.30 Bypass ≈ Packet Storm](#)
- [Public disclosure on CVE-2020-8818 \[Unauthorized Payments Hijacking + Order Status Spoofing\] · Issue #54 · cardgate/magento2 · GitHub](#)
- [Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass - PHP webapps Exploit](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

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](#)