



CVE-2020-23839

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

Summary

CVE	CVE-2020-23839
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-01 17:15:00 UTC
Updated	2022-12-03 14:56:00 UTC
Description	A Reflected Cross-Site Scripting (XSS) vulnerability in GetSimple CMS v3.3.16, in the admin/index.php login portal webpag

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Get-simple	Getsimple Cms	3.3.16	All	All	All
Application	Get-simple	Getsimple Cms	3.3.16	All	All	All

References

Reference

- [GetSimple CMS 3.3.16 Cross Site Scripting / Shell Upload ≈ Packet Storm](#)
- [GetSimple CMS 3.3.16 - Reflected XSS to RCE - PHP webapps Exploit](#)
- [Reflected Cross-Site Scripting \(XSS\) vulnerability in GetSimple CMS v3.3.16 in 'admin/index.php' · Issue #1330 · GetSimpleCMS/GetSimpleC](#)
- [GitHub - boku7/CVE-2020-23839: Public PoC Disclosure for CVE-2020-23839 - GetSimple CMS v3.3.16 suffers from a Reflected XSS on the](#)
- [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](#).

Free CVE JSON API [cve.report/api](#)

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