



CVE-2020-15155

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

Summary

CVE	CVE-2020-15155
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-28 22:15:00 UTC
Updated	2020-09-03 14:22:00 UTC
Description	basercms 4.3.6 and earlier is affected by Cross Site Scripting (XSS) via arbitrary script execution. Admin access is required.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Basercms	Basercms	All	All	All	All

References

Reference	Source
Cross Site Scripting(XSS) Vulnerability in Latest Release 4.3.6 Site basic settings · Advisory · baserproject/basercms · GitHub	CONFIRM
2020/08/27 コードインジェクション、XSSの脆弱性	MISC
Merge pull request from GHSA-4r3m-j6x5-48m3 · baserproject/basercms@94cbfab · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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