



CVE-2019-12460

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

Summary

CVE	CVE-2019-12460
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-30 14:29:00 UTC
Updated	2020-06-23 02:15:00 UTC
Description	Web Port 1.19.1 allows XSS via the /access/setup type parameter.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webport	Web Port	1.19.1	All	All	All
Application	Webport	Web Port	1.19.1	All	All	All

References

Reference

[emreovunc.com/blog/en/WebPort-Reflected-XSS-01.png](#)

[WebPort 1.19.1 Cross Site Scripting ≈ Packet Storm](#)

[GitHub - EmreOvunc/WebPort-v1.19.1-Reflected-XSS: CVE-2019-12460|Reflected XSS in WebPort-v1.19.1 impacts users who open a malicious link](#)

[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.

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