



CVE-2017-6908

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

Summary

CVE	CVE-2017-6908
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-15 00:59:00 UTC
Updated	2017-03-22 13:38:00 UTC
Description	An issue was discovered in concrete5 <= 5.6.3.4. The vulnerability exists due to insufficient filtration of user-supplied data (i

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Concrete5	Concrete5	All	All	All	All

References

Reference	Source	Link
concrete5 – Cross-Site Scripting (XSS) in “selector_data.php” · Issue #1948 · concrete5/concrete5-legacy · GitHub	CONFIRM	github.com
Fix #1948 · concrete5/concrete5-legacy@62046f5 · GitHub	CONFIRM	github.com
concrete5 Multiple Cross Site Scripting Vulnerabilities	BID	www.securi
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report