



CVE-2020-8788

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

Summary

CVE	CVE-2020-8788
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-07 14:15:00 UTC
Updated	2020-02-11 19:48:00 UTC
Description	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName p

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synaptivemedical	Clearcanvas	3.0	alpha	All	All
Application	Synaptivemedical	Clearcanvas	3.0	alpha	All	All

References

Reference	S
Cross-site Scripting (XSS) and HTML Injection on ClearCanvas ImageServer 3.0 Alpha · Issue #227 · ClearCanvas/ClearCanvas · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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

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