



CVE-2020-13893

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

Summary

CVE	CVE-2020-13893
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-18 19:15:00 UTC
Updated	2020-10-27 17:27:00 UTC
Description	Multiple stored cross-site scripting (XSS) vulnerabilities in Sage EasyPay 10.7.5.10 allow authenticated attackers to inject a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sage	Easypay	10.7.5.10	All	All	All
Application	Sage	Easypay	10.7.5.10	All	All	All

References

Reference	Source	Link	Tags
Sage Easypay Sage Singapore	MISC	www.sage.com	Product, Vendor
Multiple stored cross-site scripting (XSS) vulnerabilities in Sage EasyPay 10.7.5.10 · GitHub	MISC	gist.github.com	Third Party Advi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

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](#)