



CVE-2017-14498

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

Summary

CVE	CVE-2017-14498
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-15 18:29:00 UTC
Updated	2017-11-02 16:39:00 UTC
Description	SilverStripe CMS before 3.6.1 has XSS via an SVG document that is mishandled by (1) the Insert Media option in the conte

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
[SS-2017-017] FIX SVG uploads disabled by default · silverstripe/silverstripe-installer@c25478b · GitHub	MISC	github.com
full-disclosure - [FD] SEC Consult SA-20170914-1 :: Persistent Cross-Site Scripting in SilverStripe CMS	MISC	lists.openwall.net
3.6.1 Silverstripe CMS Documentation	MISC	docs.silverstripe.o
[SS-2017-017] FIX SVG uploads disabled by default · silverstripe/silverstripe-framework@25b77a2 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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