



CVE-2017-6877

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

Summary

CVE	CVE-2017-6877
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-14 09:59:00 UTC
Updated	2017-03-16 01:59:00 UTC
Description	Cross-site scripting (XSS) vulnerability in SVG file handling in Lutim 0.7.1 and earlier allows remote attackers to inject arbitr

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lutim Project	Lutim	All	All	All	All

References

Reference	Source	Link	Tag
Lutim CVE-2017-6877 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	
Force download if image is SVG (4c0df8f8) · Commits · Fiat Tux / Hat softwares / Lutim · GitLab	CONFIRM	framagit.org	Issu
XSS vulnerability using SVG image (#38) · Issues · Fiat Tux / Hat softwares / Lutim · GitLab	CONFIRM	framagit.org	Issu
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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