



CVE-2015-9229

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

Summary

CVE	CVE-2015-9229
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-12 22:29:00 UTC
Updated	2020-11-10 19:40:00 UTC
Description	In the nggallery-manage-gallery page in the Photocrati NextGEN Gallery plugin 2.1.15 for WordPress, XSS is possible for r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagely	Nextgen Gallery	2.1.15	All	All	All
Application	Imagely	Nextgen Gallery	2.1.15	All	All	All

References

Reference	Source
CVE-2015-9229 - Reflected Cross-Site Scripting (XSS) in NextGEN Gallery	MIS
Multiple Cross site Scripting (XSS) in NextGEN Gallery by Photocrati Version 2.1.15 · Issue #5 · cybersecurityworks/Disclosed · GitHub	MIS
CVE Program record	CVE
NVD vulnerability detail	NVD

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