CVE-2020-35943

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-35943
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-09 18:15:00 UTC
Updated	2021-02-12 15:23:00 UTC
Description	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Severe Vulnerabilities Patched in NextGen Gallery Affect over 800,000 WordPress Sites	MISC	www.wordfence.com	Exploit, Third I
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730053 Wordpress NextGen Gallery plugin Multiple Vulnerabilities

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report