



CVE-2021-32828

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-32828
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-05 23:15:00 UTC
Updated	2023-01-11 20:40:00 UTC
Description	The Nuxeo Platform is an open source content management platform for building business applications. In version 11.5.109

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hyland	Nuxeo	All	All	All	All

References

Reference

GHSL-2021-072: Reflected Cross-Site Scripting (XSS) leading to Remote Code Execution (RCE) in Nuxeo - CVE-2021-32828 | GitHub Security

nuxeo/OAuth2Callback.java at master · nuxeo/nuxeo · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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