CVE-2019-20174

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-20174
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-03 18:15:00 UTC
Updated	2020-02-05 21:01:00 UTC
Description	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auth0	Lock	All	All	All	All
Application	Auth0	Lock	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2019-20174: Security Update for Auth0 Lock Library	CONFIRM	auth0.com	Exploit, Vendor Advisory
Release v11.21.0 · auth0/lock · GitHub	MISC	github.com	Release Notes, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981600 Nodejs (npm) Security Update for auth0-lock (GHSA-w2pf-g6r8-pg22)

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