



CVE-2018-6874

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

Summary

CVE	CVE-2018-6874
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-04 17:29:00 UTC
Updated	2018-05-15 18:08:00 UTC
Description	CSRF exists in the Auth0 authentication service through 14591 if the Legacy Lock API flag is enabled.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auth0	Auth0.js	All	All	All	All

References

Reference	Source	Link	Tags
Multiple Auth0 Libraries Cross-Site Request Forgery and Authentication Bypass Vulnerabilities	BID	www.securityfocus.com	Third
Auth0 Security Bulletin CVE 2018-6874	MISC	auth0.com	Vend
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980804 Nodejs (npm) Security Update for auth0-js (GHSA-wv26-rj8c-4r33)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)