CVE-2017-9394

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

Summary

CVE	CVE-2017-9394
State	PUBLIC
Assigner	vuln@ca.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-14 21:29:00 UTC
Updated	2019-10-09 23:30:00 UTC
Description	A stored cross-site scripting vulnerability in CA Identity Governance 12.6 allows remote authenticated attackers to display H

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ca	Identity Governance	12.6.0	All	All	All
Application	Ca	Identity Governance	12.6.0	All	All	All

References

Reference	Source	Link	Tags
CA Identity Governance CVE-2017-9394 HTML Injection Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Ent
CA20171114-01: Security Notice for CA Identity Governance	CONFIRM	support.ca.com	Vendor 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.

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

Free CVE JSON API cve.report/api

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