



CVE-2019-7394

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-7394
State	PUBLIC
Assigner	vuln@ca.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-28 19:29:00 UTC
Updated	2020-10-06 14:29:00 UTC
Description	A privilege escalation vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, E

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ca	Risk Authentication	3.1	All	All	All
Application	Ca	Risk Authentication	9.0	All	All	All
Application	Ca	Risk Authentication	3.1	All	All	All
Application	Ca	Risk Authentication	9.0	All	All	All
Application	Ca	Risk Authentication	All	All	All	All
Application	Ca	Strong Authentication	7.1	All	All	All
Application	Ca	Strong Authentication	9.0	All	All	All
Application	Ca	Strong Authentication	7.1	All	All	All
Application	Ca	Strong Authentication	9.0	All	All	All
Application	Ca	Strong Authentication	All	All	All	All

References

Reference	Source	Link
CA Risk / Strong Authentication Privilege Escalation ~ Packet Storm	MISC	packetstormsecurity.com
Full Disclosure: CA20190523-01: Security Notice for CA Risk Authentication and CA Strong Authentication	FULLDISC	seclists.org
CA20190523-01: Security Notice for CA Risk Authentication and CA Strong Authentication	CONFIRM	support.ca.com
Bugtraq: CA20190523-01: Security Notice for CA Risk Authentication and CA Strong Authentication	BUGTRAQ	seclists.org

Multiple CA Products Privilege Escalation and Information Disclosure Vulnerabilities	BID	www.securityfocus
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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