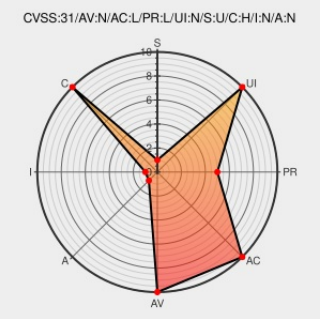
CVE-2021-44050

Published on: Not Yet Published

Last Modified on: 12/06/2021 05:20:00 PM UTC

CVE-2021-44050

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ca Network Flow Analysis from Broadcom contain the following vulnerability:

CA Network Flow Analysis (NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data.

CVE-2021-44050 has been assigned by vuln@ca.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Broadcom Support Portal	support.broadcom.com text/html	MISC support.broadcom.com/external/content/security-advisories/CA20211201-01-Security-Notice-for-CA-Network-Flow-Analysis/19689
Full Disclosure: CA20211201-01: Security	seclists.org	FULLDISC 20211203 CA20211201-01: Security Notice for CA

Notice for CA Network Flow Analysis text/html Network Flow Analysis

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Ca Network Flow Analysis	All	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

cpe:2.3:a:broadcom:ca_network_flow_analysis:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-44050 : CA Network Flow Analysis NFA 21.2.1 and earlier contain a SQL injection vulnerability in the NFA… twitter.com/i/web/status/1…	2021-12-02 19:02:28
@CyberIQs_	Technical Advisory – Authenticated SQL Injection in SOAP R cyberiqs.com/technical-advi… #infosec #infosecurity… twitter.com/i/web/status/1…	2021-12-02 20:01:27
/r/netcve	CVE-2021-44050	2021-12-02 20:38:12

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

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