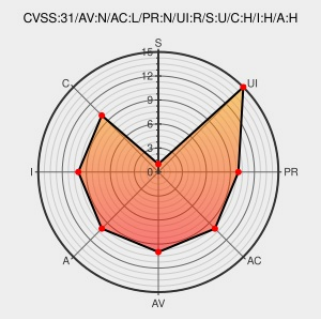
CVE-2019-18346

Published on: 12/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:06 PM UTC

CVE-2019-18346

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



Certain versions of Davical from Davical contain the following vulnerability:

A CSRF issue was discovered in DAViCal through 1.1.8. If an authenticated user visits an attacker-controlled webpage, the attacker can send arbitrary requests in the name of the user to the application. If the attacked user is an administrator, the attacker could for example add a new admin user.

CVE-2019-18346 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Bugtraq: [SECURITY] [DSA 4582-1] davical security update	seclists.org text/html	BUGTRAQ 20191216 [SECURITY] [DSA 4582-1] davical security update
DAViCal CalDAV Server 1.1.8 Cross Site Request Forgery	Third Party Advisory	MISC

≈ Packet Storm	Third Party Advisory packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155629/DAViCal-CalDAV-Server-1.1.8-Cross-Site-Request-Forgery.html
[SECURITY] [DLA 2034-1] davical security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20191214 [SECURITY] [DLA 2034-1] davical security update
DAViCal - DAViCal Home	Product www.davical.org text/html	MISC www.davical.org/
ChangeLog · master · DAViCal Project / DAViCal · GitLab	Release Notes Third Party Advisory gitlab.com text/html	MISC gitlab.com/davical-project/davical/blob/master/ChangeLog
Full Disclosure: CVE-2019-18345 Reflected Cross-Site Scripting (XSS) vulnerability in DAViCal CalDAV Server	Third Party Advisory seclists.org text/html	FULLDISC 20191210 CVE-2019-18345 Reflected Cross-Site Scripting (XSS) vulnerability in DAViCal CalDAV Server
Full Disclosure: CVE-2019-18347 Persistent Cross-Site Scripting (XSS) vulnerability in DAViCal CalDAV Server	Third Party Advisory seclists.org text/html	FULLDISC 20191210 CVE-2019-18347 Persistent Cross-Site Scripting (XSS) vulnerability in DAViCal CalDAV Server
CVE-2019-18346 Cross-Site Request Forgery (CSRF) vulnerability in DAViCal CalDAV Server – HackDefense	Exploit Third Party Advisory hackdefense.com text/html	MISC hackdefense.com/publications/cve-2019-18346-davical-caldav-server-vulnerability/
Debian -- Security Information -- DSA-4582-1 davical	www.debian.org Depreciated Link text/html	DEBIAN DSA-4582
Full Disclosure: CVE-2019-18346 Cross-Site Request Forgery (CSRF) vulnerability in DAViCal CalDAV Server	Third Party Advisory seclists.org text/html	FULLDISC 20191210 CVE-2019-18346 Cross-Site Request Forgery (CSRF) vulnerability in DAViCal CalDAV Server

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Davical	Davical	All	All	All	All

cpe:2.3:a:davical:davical:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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