

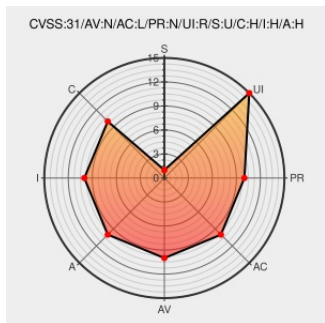


CVE-2019-18346

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 [M](#) 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

DAViCal CalDAV Server 1.1.8 Cross Site Request Forgery ≈ Packet Storm	Third Party Advisory packetstormsecurity.com text/html	📄 INFO 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 Deprecated 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

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	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→

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](#)