CVE-2019-18345

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-18345
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-12 14:15:00 UTC
Updated	2023-02-01 19:51:00 UTC
Description	A reflected XSS issue was discovered in DAViCal through 1.1.8. It echoes the action parameter without encoding. If a user

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Davical	Davical	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source	Link
Bugtraq: [SECURITY] [DSA 4582-1] davical security update	BUGTRAQ	seclists.org
[SECURITY] [DLA 2034-1] davical security update	MLIST	lists.debian.or
DAViCal - DAViCal Home	MISC	www.davical.c
ChangeLog · master · DAViCal Project / DAViCal · GitLab	MISC	gitlab.com
DAViCal CalDAV Server 1.1.8 Reflective Cross Site Scripting ≈ Packet Storm	MISC	packetstormse
Davical	MISC	wiki.davical.or
Debian -- Security Information -- DSA-4582-1 davical	DEBIAN	www.debian.o
CVE-2019-18345 Reflected Cross-Site Scripting (XSS) vulnerability in DAViCal CalDAV Server – HackDefense	MISC	hackdefense.c
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 and Source URL Uptime Status status.cve.report