



CVE-2023-27576

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-27576
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-18 15:15:00 UTC
Updated	2023-11-06 06:15:00 UTC
Description	An issue was discovered in phpList before 3.6.14. Due to an access error, it was possible to manipulate and edit data of the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phplist	Phplist	3.6.12	All	All	All

References

Reference	Source	Link
disallow non-Superusers to manage admins by michield · Pull Request #986 · phpList/phplist3 · GitHub	MISC	github.com
CVE-2023-27576 / Hacking Phplist: How I Gained Super Admin Access by Dan Barros (cupc4k3) Medium	MISC	cupc4k3.lol
phpList 3.6.14 released: security release Open Source newsletter software phpList.org	CONFIRM	www.phplist.org
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.

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](#).

Free CVE JSON API cve.report/api

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