



CVE-2023-40577

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

Summary

CVE	CVE-2023-40577
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-25 01:15:00 UTC
Updated	2023-10-24 17:49:00 UTC
Description	Alertmanager handles alerts sent by client applications such as the Prometheus server. An attacker with the permission to p

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Prometheus	Alertmanager	0.25.0	All	All	All

References

Reference	Source	Link
Alertmanager UI is vulnerable to stored XSS via the /api/v1/alerts endpoint · Advisory · prometheus/alertmanager · GitHub	MISC	gith
[SECURITY] [DLA 3609-1] prometheus-alertmanager security update	MISC	lists
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[505981](#) Alpine Linux Security Update for alertmanager

[6000105](#) Debian Security Update for prometheus-alertmanager (DLA 3609-1)

[755758](#) SUSE Enterprise Linux Security Update for golang-github-prometheus-alertmanager (SUSE-SU-2024:0512-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)