



CVE-2023-26047

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-26047
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-03 23:15:00 UTC
Updated	2023-03-10 15:03:00 UTC
Description	teler-waf is a Go HTTP middleware that provides teler IDS functionality to protect against web-based attacks. In teler-waf p

Risk And Classification

Problem Types: CWE-79 | CWE-692 | CWE-80

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kitabisa	Teler-waf	All	All	All	All

References

Reference
Bypass of IE Octal/Hex/Unicode Entities Detection in Common Web Attack Threat Rule with Case-Sensitive Entities Payload and Special Cha
Release v0.2.0 · kitabisa/teler-waf · GitHub
feat: Added case-insensitivity detects the IE octal/hex/unicode entities · dwiswant0/cwa-filter-rules@d818d16 · GitHub
CVE Program record
NVD vulnerability detail

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