CRACKEN

Vulnerability Status Report

This report lists the analysis results for the release. It is not a conformity assessment or legal advice.

Project: Edge Gateway
Release: 3.0
Responsible team: Example Org
Manufacturer: not recorded
Our role: Not recorded
Market status: released
Analysis run:
Run finished: 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC
SBOM file: edge-gateway-3.0.cdx.json
Generated: 2026-11-21 17:04:59 CET (Europe/Berlin) | 2026-11-21 16:04:59 UTC
Vulnerability matching: Completed
Matching coverage: Matching run completed; components with a supported package URL checked against OSV (including the GitHub Advisory Database), without an NVD cross-check; not run because they were not applicable: NVD (no eligible components for this source). A completed run does not mean every vulnerability source covered every component.

Executive summary

Metric	Value
Components in SBOM	5
Total findings	14
Open / in review findings	14
Findings mitigated, risk accepted or not applicable	0

Component inventory

Findings column: findings that are mitigated, accepted risk or not applicable, out of all findings.

Component	Version	Status	Findings	Description
edge-gateway-firmware [package]	3.0.0	No findings	0 / 0	Kind: package
minimist [package]	1.2.5	Open	0 / 1	Kind: package · PURL: pkg:npm/minimist@1.2.5
tokio [package]	1.7.0	Open	0 / 5	Kind: package · PURL: pkg:cargo/tokio@1.7.0
log4j-core [package]	2.14.0	Open	0 / 7	Kind: package · PURL: pkg:maven/org.apache.logging.log4j/log4j-core@2.14.0
PyYAML [package]	5.3.1	Open	0 / 1	Kind: package · PURL: pkg:pypi/pyyaml@5.3.1

Vulnerabilities and remediation actions

Component	Advisory	Severity	Status	Summary	Last action	Workflow history
log4j-core @ 2.14.0	osv: CVE-2021-44228 NVD	Critical	Open	Remote code injection in Log4j	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.

Component	Advisory	Severity	Status	Summary	Last action	Workflow history
log4j-core @ 2.14.0	osv: CVE-2021-45046 NVD	Critical	Open	Incomplete fix for Apache Log4j vulnerability	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
minimist @ 1.2.5	osv: CVE-2021-44906 NVD	Critical	Open	Prototype Pollution in minimist	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
PyYAML @ 5.3.1	osv: CVE-2020-14343 GitHub Advisory NVD	Critical	Open	Improper Input Validation in PyYAML	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
tokio @ 1.7.0	osv: CVE-2021-45710 NVD	High	Open	Race Condition in tokio	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
log4j-core @ 2.14.0	osv: CVE-2021-44832 NVD	Medium	Open	Improper Input Validation and Injection in Apache Log4j2	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
log4j-core @ 2.14.0	osv: CVE-2021-45105 NVD	Medium	Open	Apache Log4j2 vulnerable to Improper Input Validation and Uncontrolled Recursion	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
log4j-core @ 2.14.0	osv: CVE-2025-68161 NVD	Medium	Open	Apache Log4j does not verify the TLS hostname in its Socket Appender	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
log4j-core @ 2.14.0	osv: CVE-2026-34477 NVD	Medium	Open	Apache Log4j Core: `verifyHostName` attribute silently ignored in TLS configuration	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
log4j-core @ 2.14.0	osv: CVE-2026-34480 NVD	Medium	Open	Apache Log4j Core: Silent log event loss in XmlLayout due to unescaped XML 1.0 forbidden characters	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
tokio @ 1.7.0	osv: CVE-2021-38191 NVD	Medium	Open	Race condition in tokio	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.

Component	Advisory	Severity	Status	Summary	Last action	Workflow history
tokio @ 1.7.0	osv: CVE-2023-22466 GitHub Advisory NVD	Medium	Open	Tokio reject_remote_clients configuration may get dropped when creating a Windows named pipe	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
tokio @ 1.7.0	osv: GHSA-rr8g-9fpq-6wmg GitHub Advisory	Low	Open	Tokio broadcast channel calls clone in parallel, but does not require `Sync`	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.
tokio @ 1.7.0	osv: GHSA-4q83-7cq4-p6wg GitHub Advisory	Unknown	Open	`tokio::io::ReadHalf<T>::unsplit` is Unsound	Open - Discovered 2026-10-19 15:18:43 CEST (Europe/Berlin) | 2026-10-19 13:18:43 UTC	No recorded workflow actions.

Data sources

EUVD identifiers and known-exploited records: European Union Agency for Cybersecurity (ENISA), European Vulnerability Database (euvd.enisa.europa.eu). ENISA does not endorse this product.

Advisory data from OSV (osv.dev), including the GitHub Advisory Database, licensed under CC BY 4.0; some OSV sources publish under their own open licenses, listed at osv.dev.

This product uses the NVD API but is not endorsed or certified by the NVD.

CVE records from the CVE Program (cve.org); known-exploited status from the CISA KEV catalog; exploit prediction scores from FIRST EPSS (first.org/epss).