CYBER RESILIENCE ACT · ARTICLE 14 · ANNEX I PART II

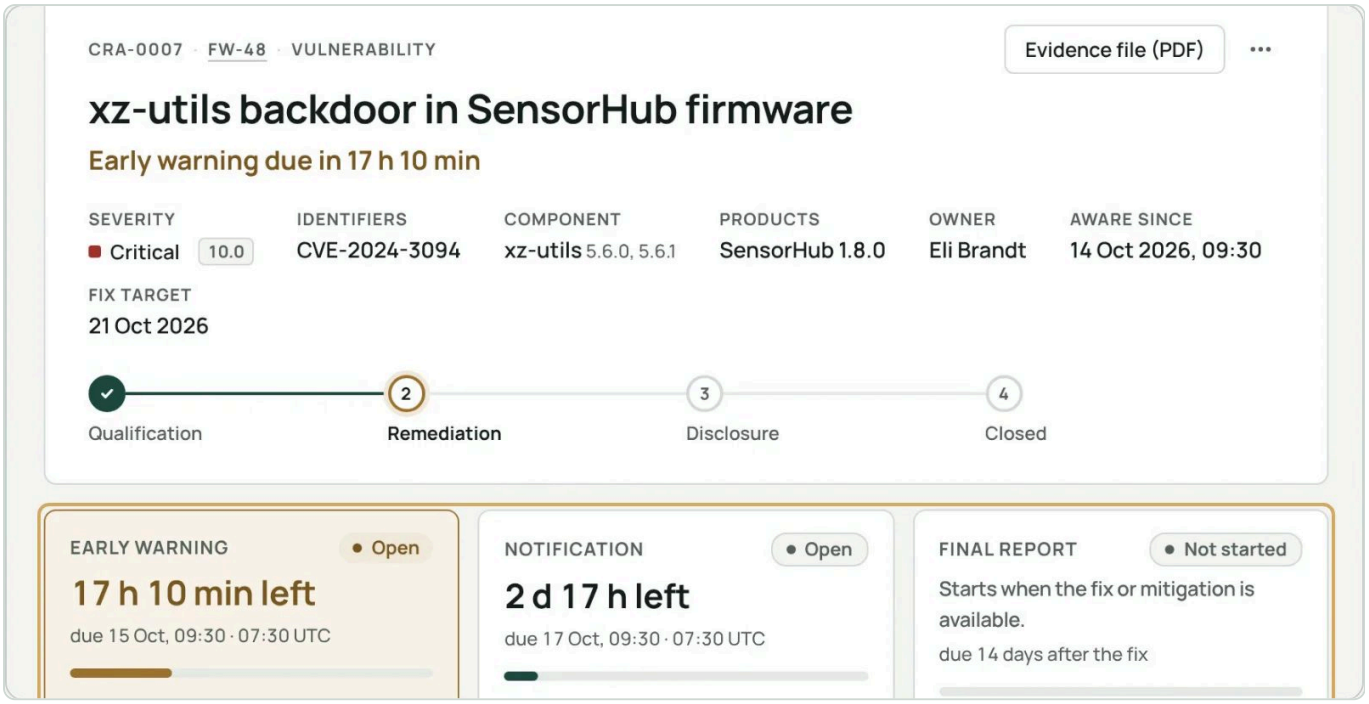
An actively exploited vulnerability, reported from Jira

One vulnerability followed step by step, with screenshots of the real app (demo data). No meeting needed: read it at your own pace, then try it on your own Jira site.

Step 1

Three clocks: the first two start from the moment you knew

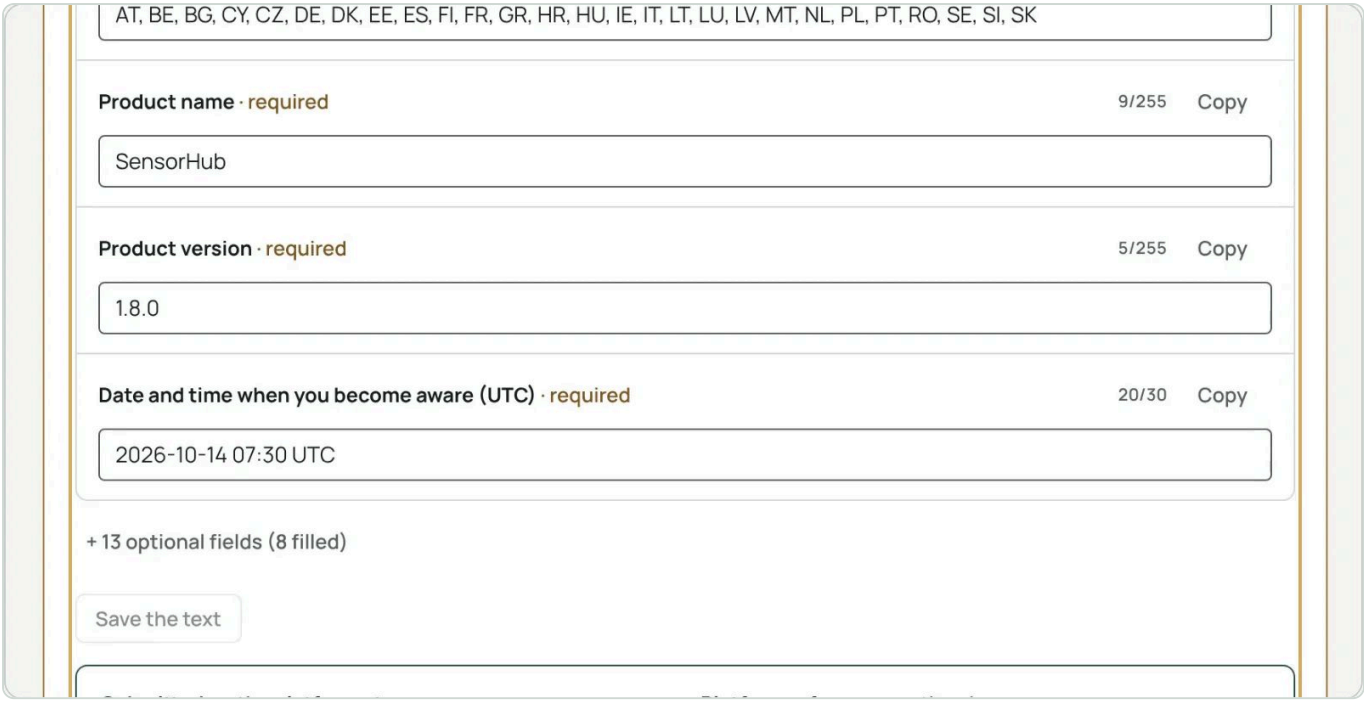
A signed, dated qualification records whether the vulnerability is actively exploited, or the incident severe, and when you became aware of it. From then on, the app counts down the early warning and the notification. The final report is due 14 days after a fix or mitigation is available.



Step 2

ENISA fields, ready to paste

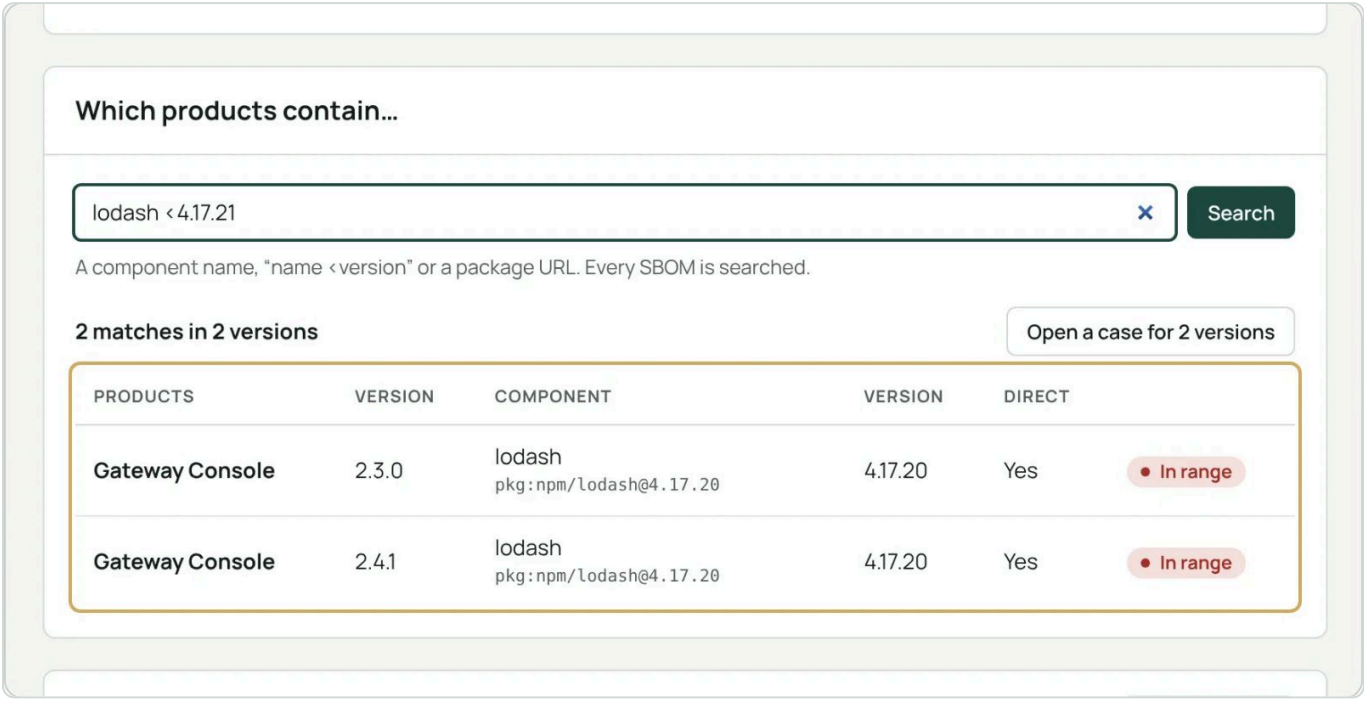
ENISA's single reporting platform currently offers no API for submissions. For each report, the app prepares every field with the platform's own label and length limit, marks what is required, and lets you copy them one by one or all at once. It never submits anything on your behalf.



Step 3

Which products ship this component?

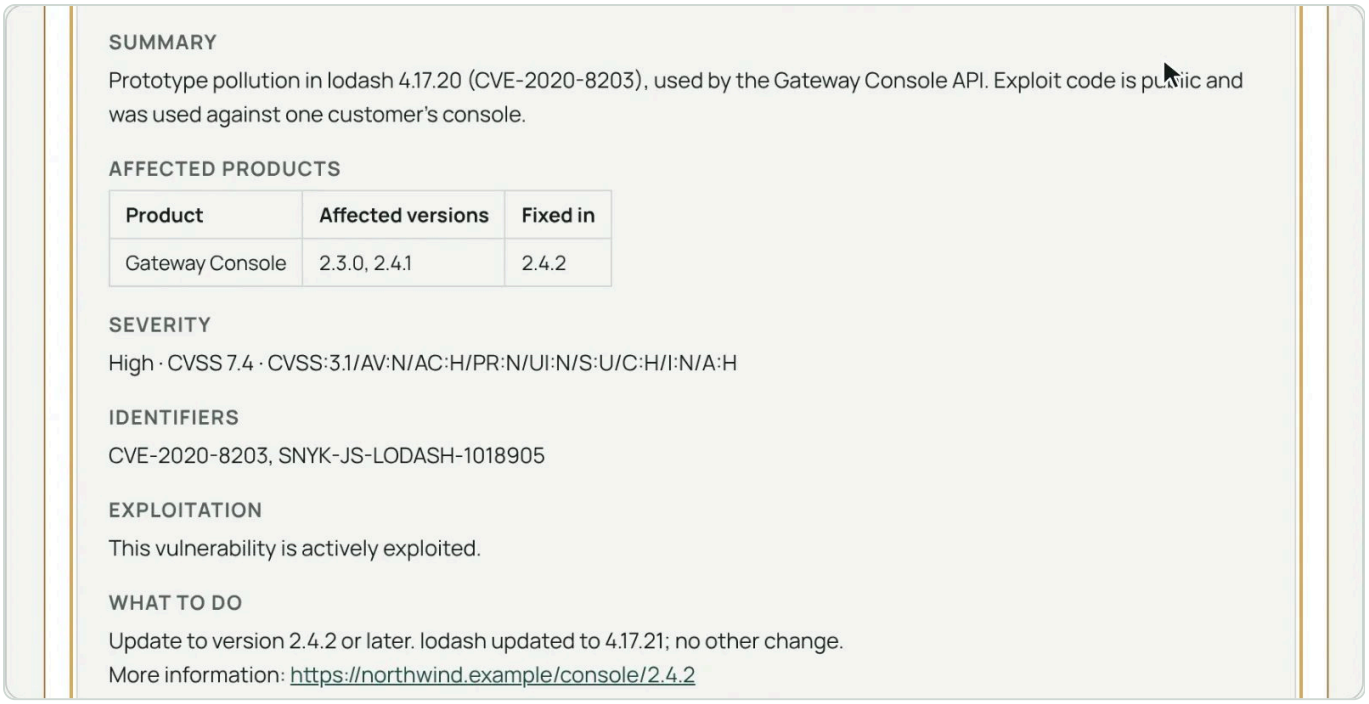
Import a CycloneDX or SPDX JSON file for each version, then search a component or a package URL: every SBOM is searched, the version range is checked, and one click opens a case for all the versions found.



Step 4

Fix, users informed, advisory

Record the security update or mitigation, inform users (Article 14(8)) with a notice prefilled from the case, and publish a security advisory with a CSAF 2.0 file built from the record.



SUMMARY

Prototype pollution in lodash 4.17.20 (CVE-2020-8203), used by the Gateway Console API. Exploit code is public and was used against one customer's console.

AFFECTED PRODUCTS

Product	Affected versions	Fixed in
Gateway Console	2.3.0, 2.4.1	2.4.2

SEVERITY

High · CVSS 7.4 · CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

IDENTIFIERS

CVE-2020-8203, SNYK-JS-LODASH-1018905

EXPLOITATION

This vulnerability is actively exploited.

WHAT TO DO

Update to version 2.4.2 or later. lodash updated to 4.17.21; no other change.
More information: https://northwind.example/console/2.4.2

Try it on your own site: Clearlane CRA has a free trial on the Atlassian Marketplace. Want this walkthrough written for your own process? Write to **maxime@clearlaneapps.com**. The first-24-hours template and the supplier file: **clearlaneapps.com/solutions/cyber**.