CERT-EU

Security Advisory 2023-013

Critical SQL injection vulnerabilities in MISP

February 21, 2023 — v1.0

TLP:CLEAR

History:

- *21/02/2023 — v1.0 – Initial publication*

Summary

On February 20, 2023, the MISP project team released advisories regarding 2 critical SQL injection vulnerabilities in MISP Threat Intelligence and Sharing Platform [1]. The team decided to follow a silent fix procedure, releasing several updates in November and December 2022, giving enough time to users to update their instances to a safe version.

Technical Details

CVE-2022-48329

The MISP platform allowed users to provide custom field ordering for certain endpoints such as RestSearch. These ordering were set using URL parameters in the format of `/order:field_name`. However, the `order` parameter of the CakePHP `find()` function is not SQLi safe and thus, the MISP project team has introduced field allow-listing for any occurrence of custom order fields. Any sorting relying on `/sort:field_name/direction:asc|desc` is unaffected and safe [2].

CVE-2022-48328

The `CRUD` component of the MISP platform would allow for custom search parameters to be passed - and whilst the lookup values are SQLi safe and properly sanitised, the field names themselves are not. With some clever forged requests, these can be abused [2].

Affected Products

CVE-2022-48329 [2]:

- MISP before v2.4.166;

CVE-2022-48328 [2]:

- MISP before v2.4.167;

Recommendations

As the project team released the version `2.4.167` on December 22, 2022, most of the MISP instances should be safe already. Nevertheless, CERT-EU recommends checking running MISP instance versions, and updating MISP Threat Intelligence and Sharing Platform to the latest version, when applicable, as soon as possible.

References

[1] https://www.misp-project.org/security/

[2] https://www.misp-project.org/2023/02/20/Critical_SQL_Injection_Vulnerabilities_Fixed.html/