

Overall Rating - High



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware PHP could allow a remote attacker to obtain sensitive information, caused by insufficient validation of user-supplied XML input.

Platforms Affected:

- PHP 8.1.21
- PHP 8.0.29

Technical Details

CVE-2023-3823 is an information disclosure vulnerability that could allow a remote attacker to obtain sensitive information from a PHP application. The vulnerability is caused by insufficient validation of user-supplied XML input. An attacker could exploit this vulnerability by sending a specially crafted XML code to the application. The code would then be parsed by the application, and the attacker could gain access to sensitive information, such as the contents of arbitrary files on the system or the results of external requests. Every application, library, and server parsing or interacting with XML documents is susceptible to this flaw.

This vulnerability is rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-3823
- https://vulners.com/nessus/PHP_8_1_22.NASL