



CVE-2023-29530

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

Summary

CVE	CVE-2023-29530
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-24 20:15:00 UTC
Updated	2023-05-05 13:58:00 UTC
Description	Laminas Diactoros provides PSR HTTP Message implementations. In versions 2.18.0 and prior, 2.19.0, 2.20.0, 2.21.0, 2.22.0, 2.23.0, 2.24.0, and 2.25.0, the PSR Message implementation was vulnerable to a Denial of Service (DoS) attack. An attacker could send a request with a header name that is longer than the allowed limit, causing the application to crash. This vulnerability affects all versions of Laminas Diactoros that use the PSR Message implementation.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Getlaminas	Laminas-diactoros	All	All	All	All
Application	Getlaminas	Laminas-diactoros	2.19.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.20.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.21.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.22.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.23.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.24.0	All	All	All
Application	Getlaminas	Laminas-diactoros	2.25.0	All	All	All
Application	Guzzlephp	Psr-7	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: php-laminas-diactoros2-2.25.2-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Improper header name validation in guzzlehttp/psr7 · CVE-2023-29197 · GitHub Advisory Database · GitHub	MISC	github.com
HTTP Multiline Header Termination · Advisory · laminas/laminas-diactoros · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

284168 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2023-8cf8786a16)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)