



CVE-2021-3007

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

Summary

CVE	CVE-2021-3007
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-04 03:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	** DISPUTED ** Laminas Project laminas-http before 2.14.2, and Zend Framework 3.0.0, has a deserialization vulnerability

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Getlaminas	Laminas-http	All	All	All	All
Application	Getlaminas	Laminas-http	All	All	All	All
Application	Zend	Zend Framework	3.0.0	All	All	All
Application	Zend	Zend Framework	3.0.0	All	All	All

References

Reference

- [History for src/Response/Stream.php - laminas/laminas-http · GitHub](#)
- [Security tightening: verify a stream file name is a string before unlinking by weierophinney · Pull Request #48 · laminas/laminas-http · GitHub](#)
- [FreakOut – Leveraging Newest Vulnerabilities for creating a Botnet - Check Point Research](#)
- [Release 2.14.2 · laminas/laminas-http · GitHub](#)
- [zendframework3-/zend framework3 反序列化 rce.md at main · Ling-Yizhou/zendframework3- · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)