



CVE-2016-10034

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

Summary

CVE	CVE-2016-10034
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-30 19:59:00 UTC
Updated	2018-10-21 10:29:00 UTC
Description	The setFrom function in the Sendmail adapter in the zend-mail component before 2.4.11, 2.5.x, 2.6.x, and 2.7.x before 2.7.1

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zend	Zend-mail	2.5.0	All	All	All
Application	Zend	Zend-mail	2.5.1	All	All	All
Application	Zend	Zend-mail	2.5.2	All	All	All
Application	Zend	Zend-mail	2.6.0	All	All	All
Application	Zend	Zend-mail	2.6.1	All	All	All
Application	Zend	Zend-mail	2.6.2	All	All	All
Application	Zend	Zend-mail	2.7.0	All	All	All
Application	Zend	Zend-mail	2.7.1	All	All	All
Application	Zend	Zend-mail	2.5.0	All	All	All
Application	Zend	Zend-mail	2.5.1	All	All	All
Application	Zend	Zend-mail	2.5.2	All	All	All
Application	Zend	Zend-mail	2.6.0	All	All	All
Application	Zend	Zend-mail	2.6.1	All	All	All
Application	Zend	Zend-mail	2.6.2	All	All	All
Application	Zend	Zend-mail	2.7.0	All	All	All
Application	Zend	Zend-mail	2.7.1	All	All	All
Application	Zend	Zend-mail	All	All	All	All

Application	Zend	Zend Framework	All	All	All	All
-------------	----------------------	--------------------------------	-----	-----	-----	-----

References

Reference

- [PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution - PHP webapps Exploit](#)
- [Zend Framework - Advisory](#)
- [Zend Framework: Multiple vulnerabilities \(GLSA 201804-10\) — Gentoo security](#)
- [Zend Framework / zend-mail < 2.4.11 - Remote Code Execution - PHP webapps Exploit](#)
- [ZendFramework-Exploit-ZendMail-Remote-Code-Exec-CVE-2016-10034-Vuln](#)
- [PHPMailer < 5.2.20 / SwiftMailer < 5.4.5-DEV / Zend Framework / zend-mail < 2.4.11 - 'AIO' 'PwnScriptum' Remote Code Execution - PHP we](#)
- [Zend Framework Input Validation Flaw in zend-mail Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker](#)
- [Zend Framework 'zend-mail' Component Remote Code Execution Vulnerability](#)
- [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](#)