



CVE-2018-13981

Published on: 07/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:29 PM UTC

CVE-2018-13981

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Zeta Producer Desktop Cms](#) from [Zeta-producer](#) contain the following vulnerability:

The websites that were built from Zeta Producer Desktop CMS before 14.2.1 are vulnerable to unauthenticated remote code execution due to a default component that permits arbitrary upload of PHP files, because the formmailer widget blocks .php files but not .php5 or .phtml files. This is related to /assets/php/formmailer/SendEmail.php and /assets/php/formmailer/functions.php.

CVE-2018-13981 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Zeta Producer Desktop CMS 14.2.0 - Remote Code Execution / Local File Disclosure - PHP webapps Exploit	Exploit Third Party Advisory	EXPLOIT-DB 45016

VDB Entry
www.exploit-db.com
Proof of Concept
text/html

Remote Code Execution and Local File Disclosure in Zeta Producer Desktop CMS

Exploit
Third Party Advisory
web.archive.org
text/html
Inactive Link Not Archived

★ MISC www.sec-consult.com/en/blog/advisories/remote-code-execution-local-file-disclosure-zeta-producer-desktop-cms/

Zeta Producer Desktop CMS 14.2.0 Code Execution /
File Disclosure ≈ Packet Storm

Exploit
Third Party Advisory
VDB Entry
packetstormsecurity.com
text/html

 MISC

packetstormsecurity.com/files/148537/Zeta-Producer-Desktop-CMS-14.2.0-Code-Execution-File-Disclosure.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zeta-producer	Zeta Producer Desktop Cms	All	All	All	All
Application	Zeta-producer	Zeta Producer Desktop Cms	All	All	All	All
cpe:2.3:a:zeta-producer::zeta_producer_desktop_cms:*.*.*.*.*.*.*.*:						
cpe:2.3:a:zeta-producer::zeta_producer_desktop_cms:*.*.*.*.*.*.*.*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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](#).

CVE.report and Source URL Uptime Status status.cve.report