



CVE-2016-1230

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-1230
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-05 01:59:00 UTC
Updated	2016-06-06 18:06:00 UTC
Description	Cross-site scripting (XSS) vulnerability in NTT PC Communications WebARENA Service formmail before 2.2.1 allows remo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntt	Webarena Service Formmail	All	All	All	All

References

Reference

Suite2 フォームメール機能の脆弱性対応について | 公式 WebARENA(ウェブアリーナ) | レンタルサーバー,VPS,クラウド,メールサーバー, 専

JVNDB-2016-000072

JVN#24143619: WebARENA formmail vulnerable to cross-site scripting

Suite CGI フォームメール機能の脆弱性対応について | 公式 WebARENA(ウェブアリーナ) | レンタルサーバー,VPS,クラウド,メールサーバー

[CGI・SSI] フォームメール | 共用サーバーなら安心と信頼のWebARENA(ウェブアリーナ) | Suiteサポート

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)