CVE-2017-11466

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-11466
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-20 00:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Arbitrary file upload vulnerability in com/dotmarketing/servlets/AjaxFileUploadServlet.class in dotCMS 4.1.1 allows remote a

Risk And Classification

Primary CVSS: v3.0 7.2 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-434 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dotcms	Dotcms	4.1.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
/assets directory accessible via web request · Issue #12131 · dotCMS/core · GitHub	af854a3a-2127-422b-91ae-364da2661108	github.co
DotCMS 4.1.1 Shell Upload ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packetst
Full Disclosure: DotCMS /servlets/ajax_file_upload Arbitrary File Upload Vulnerability	af854a3a-2127-422b-91ae-364da2661108	seclists.c
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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