



CVE-2018-7600

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

Summary

CVE	CVE-2018-7600
State	PUBLIC
Assigner	security@drupal.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-29 07:29:00 UTC
Updated	2019-03-01 18:04:00 UTC
Description	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary

Risk And Classification

EPSS: 0.944890000 probability, percentile 1.000000000 (date 2026-05-08)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Known

Problem Types: CWE-20

CISA Known Exploited Vulnerability

Vendor	Drupal
Product	Drupal Core
Name	Drupal Core Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-7600

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal	All	All	All	All

Application	Drupal	Drupal	All	All	All	All
References						
Reference						
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit) - PHP remote Exploit						
Uncovering Drupalgeddon 2 - Check Point Research						
Over 100,000 Drupal websites vulnerable to Drupalgeddon 2 (CVE-2018-7600) Bad Packets Report						
Debian -- Security Information -- DSA-4156-1 drupal7						
GitHub - a2u/CVE-2018-7600: ???Proof-of-Concept for CVE-2018-7600 Drupal SA-CORE-2018-002						
Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002 Drupal.org						
Any Exploit Code For "CVE-2018-7600"						
[SECURITY] [DLA 1325-1] drupal7 security update						
JavaScript is not available.						
Drupal Core CVE-2018-7600 Multiple Remote Code Execution Vulnerabilities						
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution						
GitHub - g0rx/CVE-2018-7600-Drupal-RCE: CVE-2018-7600 Drupal RCE						
Remote Code Execution with Drupal core (SA-CORE-2018-002)						
FAQ about SA-CORE-2018-002 Drupal Groups						
JavaScript is not available.						
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC) - PHP webapps Exploit						
Drupal Core Vulnerability CVE-2018-7600 Patch Tenable®						
Synology Inc.						
Drupal Form API Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker						
aran na Twitterze: "The CVE is (obviously) coy about the actual exploit, but there's one subsystem that has been there for some ~12 years, re						
CVE Program record						
NVD vulnerability detail						
CISA Known Exploited Vulnerabilities catalog						
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
500870 Alpine Linux Security Update for drupal7						
504694 Alpine Linux Security Update for drupal7						

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