



CVE-2017-6920

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

Summary

CVE	CVE-2017-6920
State	PUBLIC
Assigner	security@drupal.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-06 15:29:00 UTC
Updated	2018-10-04 16:16:00 UTC
Description	Drupal core 8 before versions 8.3.4 allows remote attackers to execute arbitrary code due to the PECL YAML parser not ha

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal	All	All	All	All

References

Reference	Source	Link
Drupal Core - Multiple Vulnerabilities - SA-CORE-2017-003 Drupal.org	CONFIRM	www.drupal.org
Drupal Core CVE-2017-6920 Remote Code Execution Vulnerability	BID	www.securityfo
Drupal Bugs Let Remote Users Access Certain Uploaded Files and Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytr
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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