



CVE-2018-6758

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

Summary

CVE	CVE-2018-6758
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-06 18:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	The uwsgi_expand_path function in core/utils.c in Unbit uWSGI through 2.0.15 has a stack-based buffer overflow via a large

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Unbit	Uwsgi	All	All	All	All

References

Reference	Source	Link	Tags
improve uwsgi_expand_path() to sanitize input, avoiding stack corrupt... · unbit/uwsgi@cb4636f · GitHub	MISC	github.com	Pat
lists.unbit.it/pipermail/uwsgi/2018-February/008835.html	MISC	lists.unbit.it	Iss
[SECURITY] [DLA 1275-1] uwsgi security update	MLIST	lists.debian.org	Thi
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500715](#) Alpine Linux Security Update for uwsgi

[504489](#) Alpine Linux Security Update for uwsgi

© [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](#)