



# ownDMS 4.7 SQL Injection via pdfstream.php imagestream.php

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

## Summary

<b>CVE</b>	CVE-2019-25580
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-21 16:16:02 UTC
<b>Updated</b>	2026-04-15 16:49:00 UTC
<b>Description</b>	ownDMS 4.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries

## Risk And Classification

**Primary CVSS:** v4.0 8.8 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-434 | CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N
3.1	disclosure@vulncheck.com	Primary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Owndms	OwnDMS	affected 4.7	Not specified

References		
Reference	Source	Link
<a href="http://www.vulncheck.com/advisories/owndms-sql-injection-via-pdfstream-php-imagestream...">www.vulncheck.com/advisories/owndms-sql-injection-via-pdfstream-php-imagestream...</a>	disclosure@vulncheck.com	<a href="http://www.vulncheck.com">www.vulncheck.com</a>
<a href="http://datapacket.dl.sourceforge.net/project/owndms/owndms_47.zip">datapacket.dl.sourceforge.net/project/owndms/owndms_47.zip</a>	disclosure@vulncheck.com	<a href="http://datapacket.dl.sourceforge.net">datapacket.dl.sourceforge.net</a>
<a href="http://www.owndms.com">www.owndms.com</a>	disclosure@vulncheck.com	<a href="http://www.owndms.com">www.owndms.com</a>
<a href="http://www.exploit-db.com/exploits/46168">www.exploit-db.com/exploits/46168</a>	disclosure@vulncheck.com	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit  
**CNA: Ihsan Sencan (en)**

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).  
**Free CVE JSON API** [cve.report/api](http://cve.report/api)  
**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)