



CVE-2018-16405

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

Summary

CVE	CVE-2018-16405
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-03 19:29:00 UTC
Updated	2018-10-30 19:47:00 UTC
Description	An issue was discovered in Mayan EDMS before 3.0.2. The Appearance app sets window.location directly, leading to XSS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mayan-edms	Mayan Edms	All	All	All	All
Application	Mayan-edms	Mayan Edms	All	All	All	All

References

Reference	Source
HISTORY.rst · master · Mayan EDMS / Mayan EDMS · GitLab	MISC
Avoid setting window.location directly to avoid exploit of cross site... (9ebe8059) · Commits · Mayan EDMS / Mayan EDMS · GitLab	MISC
DOM based Cross Site Scripting (#494) · Issues · Mayan EDMS / Mayan EDMS · GitLab	MISC
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981102 Python (pip) Security Update for mayan-edms (GHSA-fpcv-j2q9-vqhw)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)