



CVE-2018-12941

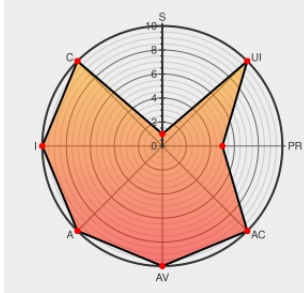
Published on: 07/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:23 PM UTC

CVE-2018-12941

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Seeddms](#) from [Seeddms](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code in SeedDMS (formerly LetoDMS and MyDMS) before 5.1.8 by adding a system command at the end of the "cacheDir" path and following usage of the "Clear Cache" functionality. This allows an authenticated attacker, with permission to the Settings functionality, to inject arbitrary system commands within the application by manipulating the "Cache directory" path. An attacker can use it to perform malicious tasks such as to extract, change, or delete sensitive information or run system commands on the underlying operating system.

CVE-2018-12941 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

seeddms / Code / [2c013b]
/CHANGELOG

Third Party Advisory

sourceforge.net

text/html

CONFIRM

sourceforge.net/p/seeddms/code/ci/seeddms-5.1.x/tree/CHANGELOG

CVE-2018-12941 | Context Information Security

Third Party Advisory

www.contextis.com

text/html

MISC

www.contextis.com/resources/advisories/cve-2018-12941

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:seeddms:seeddms:*****::

cpe:2.3:a:seeddms:seeddms:*****::

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →