



CVE-2017-16615

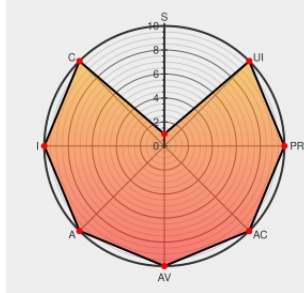
Published on: 11/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16615

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

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



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

An exploitable vulnerability exists in the YAML parsing functionality in the `parse_yaml_query` method in `parser.py` in `MLAlchemy` before 0.2.2. When processing YAML-Based queries for data, a YAML parser can execute arbitrary Python commands resulting in command execution because `load` is used where `safe_load` should have been used. An attacker can insert Python into loaded YAML to trigger this vulnerability.

CVE-2017-16615 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2017-16615: Critical RESTful Web Applications Vulnerability - Joel	Third Party Advisory joel-malwarebenchmark.github.io	MISC joel-malwarebenchmark.github.io/blog/2017/11/08/cve-2017-16615-web-applications-vulnerability/

text/html

parse_yaml_query method is vulnerable · Issue #1 · thanethomson/MLAlchemy · GitHub

Issue Tracking

github.com

text/html

CONFIRM github.com/thanethomson/MLAlchemy/issues/1

attempting to fix security flaw (issue #1) · thanethomson/MLAlchemy@bc79575 · GitHub

Issue Tracking

github.com

text/html

CONFIRM github.com/thanethomson/MLAlchemy/commit/bc795757febdcc430

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.

Related QID Numbers

980782 Python (pip) Security Update for MLAlchemy (GHSA-xpm8-98mx-h4c5)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mlalchemy Project	Mlalchemy	0.1.1	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.1.2	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.1.3	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.2.0	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.2.1	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.1.1	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.1.2	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.1.3	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.2.0	All	All	All
Application	Mlalchemy Project	Mlalchemy	0.2.1	All	All	All

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.1:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.2:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.3:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.2.0:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.2.1:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.1:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.2:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.1.3:*****:

cpe:2.3:a:mlalchemv_project:mlalchemv:0.2.0:*****:

cpe:2.3:a:mlalchemy_project:mlalchemy:0.2.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→