



CVE-2017-16618

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

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

CVE-2017-16618

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

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

An exploitable vulnerability exists in the YAML loading functionality of util.py in OwlMixin before 2.0.0a12. A "Load YAML" string or file (aka load_yaml or load_yamlf) 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-2017-16618 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
load_yaml and load_yamlf methods is vulnerable · Issue	Exploit Patch	CONFIRM github.com/tadashi-aikawa/owlmixin/issues/12

#12 · tadashi-aikawa/owlmixin · GitHub

Third Party Advisory
github.com
text/html

:scream: Fix vulnerability of
`load\_yaml` and `load\_yamlf`
(#12) · tadashi-
aikawa/owlmixin@5d05753 ·
GitHub

Patch
Third Party Advisory
github.com
text/html

CONFIRM github.com/tadashi-aikawa/owlmixin/commit/5d0575303f6df869a515ced4285f24ba721e0d4e

CVE-2017-16618: Convert
through OwlMixin - Joel

Exploit
Third Party Advisory
joel-malwarebenchmark.github.io
text/html

MISC joel-malwarebenchmark.github.io/blog/2017/11/08/cve-2017-16618-convert-through-owlmixin/

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

981133 Python (pip) Security Update for owlmixin (GHSA-ccmq-qvcp-5mrm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Owlmixin Project	Owlmixin	All	All	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha1	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha10	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha11	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha2	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha3	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha4	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha5	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha6	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha7	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha8	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha9	All	All
Application	Owlmixin Project	Owlmixin	All	All	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha1	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha10	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha11	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha2	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha3	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha4	All	All

Application	Owlmixin Project	Owlmixin	2.0.0	alpha5	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha6	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha7	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha8	All	All
Application	Owlmixin Project	Owlmixin	2.0.0	alpha9	All	All
cpe:2.3:a:owlmixin_project:owlmixin:****.*.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha1:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha10:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha11:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha2:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha3:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha4:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha5:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha6:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha7:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha8:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha9:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:****.*.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha1:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha10:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha11:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha2:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha3:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha4:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha5:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha6:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha7:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha8:****.*.*.*:						
cpe:2.3:a:owlmixin_project:owlmixin:2.0.0:alpha9:****.*.*.*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© [CVE.report](#) 2023   |

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](#)