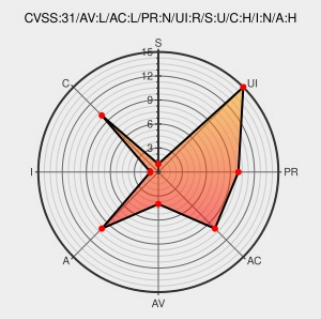
CVE-2015-8549

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8549

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pyamf from Pyamf contain the following vulnerability:

XML external entity (XXE) vulnerability in PyAMF before 0.8.0 allows remote attackers to cause a denial of service or read arbitrary files via a crafted Action Message Format (AMF) payload.

CVE-2015-8549 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.securityfocus.com/archive/1/archive/1/537151/100/0/threaded

oCERT.org - oCERT Advisories	Third Party Advisory www.ocert.org text/xml	MISC www.ocert.org/advisories/ocert-2015-011.html
Switch to use defusedxml as the default xml loader. by njoyce · Pull Request #58 · hydralabs/pyamf · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/hydralabs/pyamf/pull/58
Release v0.8.0 · hydralabs/pyamf · GitHub	Release Notes github.com text/html	MISC github.com/hydralabs/pyamf/releases/tag/v0.8.0

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	Pyamf	Pyamf	All	All	All	All
Application	Pyamf	Pyamf	All	All	All	All

cpe:2.3:a:pyamf:pyamf:*:*:*:*:*:*:*:*:

cpe:2.3:a:pyamf:pyamf:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→