

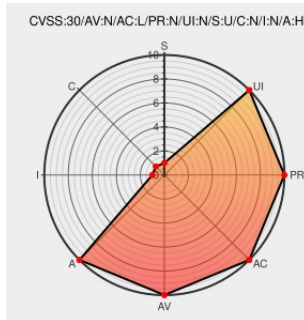


CVE-2016-6580

Published on: 01/10/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-6580

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

Certain versions of [Python Priority Library](#) from [Python](#) contain the following vulnerability:

A HTTP/2 implementation built using any version of the Python priority library prior to version 1.2.0 could be targeted by a malicious peer by having that peer assign priority information for every possible HTTP/2 stream ID. The priority tree would happily continue to store the priority information for each stream, and would therefore allocate unbounded

amounts of memory. Attempting to actually use a tree like this would also cause extremely high CPU usage to maintain the tree.

CVE-2016-6580 has been assigned by [M cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
More Found I Read the Docs	CVE-2016-6580	CONFIRM author

Mitigation

Vendor Advisory

python-hyper.org

text/html

Inactive Link Not Archived

CONFIRM python-hyper.org/priority/en/latest/security/CVE-2016-6580.html

Python priority CVE-2016-6580 Remote Denial of Service Vulnerability

Third Party Advisory

VDB Entry

cve.report (archive)

text/html

BID 92311

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	Python	Python Priority Library	1.0.0	All	All	All
Application	Python	Python Priority Library	1.1.0	All	All	All
Application	Python	Python Priority Library	1.1.1	All	All	All
Application	Python	Python Priority Library	1.0.0	All	All	All
Application	Python	Python Priority Library	1.1.0	All	All	All
Application	Python	Python Priority Library	1.1.1	All	All	All
cpe:2.3:a:python:python_priority_library:1.0.0:*:*:*:*:*:						
cpe:2.3:a:python:python_priority_library:1.1.0:*:*:*:*:*:						
cpe:2.3:a:python:python_priority_library:1.1.1:*:*:*:*:*:						
cpe:2.3:a:python:python_priority_library:1.0.0:*:*:*:*:*:						
cpe:2.3:a:python:python_priority_library:1.1.0:*:*:*:*:*:						
cpe:2.3:a:python:python_priority_library:1.1.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report