

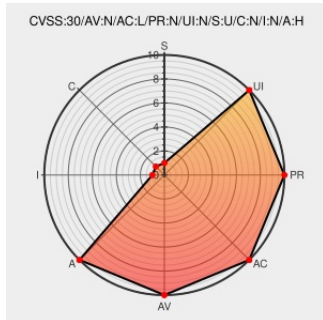


CVE-2016-6581

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

Last Modified on: 03/23/2021 11:27:12 PM UTC

CVE-2016-6581

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

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

A HTTP/2 implementation built using any version of the Python HPACK library between v1.0.0 and v2.2.0 could be targeted for a denial of service attack, specifically a so-called "HPACK Bomb" attack. This attack occurs when an attacker inserts a header field that is exactly the size of the HPACK dynamic header table into the dynamic header

table. The attacker can then send a header block that is simply repeated requests to expand that field in the dynamic table. This can lead to a gigantic compression ratio of 4,096 or better, meaning that 16kB of data can decompress to 64MB of data on the target machine.

CVE-2016-6581 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: **7.8 - HIGH**

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

CVE References

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

Maze Found | Read the Docs

Mitigation

Vendor Advisory

python-hyper.org

text/html

Inactive Link Not Archived

 CONFIRM python-hyper.org/hpack/en/latest/security/CVE-2016-6581.html

Python HPACK CVE-2016-6581 Remote Denial of Service Vulnerability

Third Party Advisory

VDB Entry

cve.report (archive)

text/html

 BID 92315

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

981106 Python (pip) Security Update for hpack (GHSA-ffq8-576r-v26g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python	Hpack	1.0	All	All	All
Application	Python	Hpack	2.0	All	All	All
Application	Python	Hpack	2.0.1	All	All	All
Application	Python	Hpack	2.1.1	All	All	All
Application	Python	Hpack	2.2	All	All	All
Application	Python	Hpack	1.0	All	All	All
Application	Python	Hpack	2.0	All	All	All
Application	Python	Hpack	2.0.1	All	All	All
Application	Python	Hpack	2.1.1	All	All	All
Application	Python	Hpack	2.2	All	All	All
Application	Python	Hyper	0.4	All	All	All
Application	Python	Hyper	0.6	All	All	All
Application	Python	Hyper	0.4	All	All	All
Application	Python	Hyper	0.6	All	All	All

cpe:2.3:a:python:hpack:1.0:*:*:*:*:*:

cpe:2.3:a:python:hpack:2.0:*:*:*:*:*:

cpe:2.3:a:python:hpack:2.0.1:*:*:*:*:*:

cpe:2.3:a:python:hpack:2.1.1:*:*:*:*:*:

cpe:2.3:a:python:hpack:2.2:*:*:*:*:*:

cpe:2.3:a:python:hpack:1.0:*****:
cpe:2.3:a:python:hpack:2.0:*****:
cpe:2.3:a:python:hpack:2.0.1:*****:
cpe:2.3:a:python:hpack:2.1.1:*****:
cpe:2.3:a:python:hpack:2.2:*****:
cpe:2.3:a:python:hyper:0.4:*****:
cpe:2.3:a:python:hyper:0.6:*****:
cpe:2.3:a:python:hyper:0.4:*****:
cpe:2.3:a:python:hyper:0.6:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)