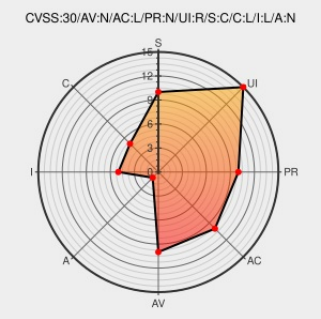
CVE-2016-5699

Published on: 09/02/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:24:00 PM UTC

CVE-2016-5699

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



Certain versions of Python from Python contain the following vulnerability:

CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.

CVE-2016-5699 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client	Mailing List, www.openwall.com, text/html	MLIST [oss-security] 20160616 Re: CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client
1303699 – (CVE-2016-5699) CVE-2016-5699	bugzilla.redhat.com	MISC bugzilla.redhat.com/show_bug.cgi?id=1303699

python: http protocol steam injection attack	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1630
CVE-2016-5699 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-5699
[SECURITY] [DLA 1663-1] python3.4 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20190207 [SECURITY] [DLA 1663-1] python3.4 security update
Python 'urrlib2/urllib/httplib/http.client' HTTP Header Injection Vulnerability	cve.report (archive) text/html	BID 91226
Changelog — Python 3.4.5 documentation	Release Notes docs.python.org text/html	CONFIRM docs.python.org/3.4/whatsnew/changelog.html#python-3-4-4
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1626
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1628
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1629
Splunk Enterprise 6.4.5 addresses multiple vulnerabilities | Splunk	www.splunk.com text/html	CONFIRM www.splunk.com/view/SP-CAAAPUE
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1630
[security-announce] openSUSE-SU-2020:0086-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0086
cpython: 1c45047c5102	Patch hg.python.org text/html	CONFIRM hg.python.org/cpython/rev/1c45047c5102
oss-security - CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client	Mailing List www.openwall.com text/html	MLIST [oss-security] 20160614 CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1628
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1629
cpython: bf3e1c9b80e9	Patch hg.python.org text/html	CONFIRM hg.python.org/cpython/rev/bf3e1c9b80e9
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1627
Blindspot Security	Exploit Third Party Advisory blog.blindspotsecurity.com text/html	MISC blog.blindspotsecurity.com/2016/06/advisory-http-header-injection-in.html
Red Hat Customer Portal	access.redhat.com	MISC access.redhat.com/errata/RHSA-2016:1626

	text/html	
oss-security - Re: CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client	Mailing List www.openwall.com text/html	MLIST [oss-security] 20160615 Re: CVE request: Python HTTP header injection in urrlib2/urllib/httplib/http.client
Splunk Enterprise 6.5.1 addresses multiple OpenSSL vulnerabilities | Splunk	www.splunk.com text/html	CONFIRM www.splunk.com/view/SP-CAAAPSV
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:1627
	Release Notes hg.python.org text/plain	CONFIRM hg.python.org/cpython/raw-file/v2.7.10/Misc/NEWS
Oracle Solaris Bulletin - July 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html

Related QID Numbers

730315 Splunk Enterprise and Light Security Update (SP-CAAAPSV) (SPL-128812)

Exploit/POC from Github

PoC code of CVE-2016-5699 Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python	Python	3.0	All	All	All
Application	Python	Python	3.0.1	All	All	All
Application	Python	Python	3.1.0	All	All	All
Application	Python	Python	3.1.1	All	All	All
Application	Python	Python	3.1.2	All	All	All
Application	Python	Python	3.1.3	All	All	All
Application	Python	Python	3.1.4	All	All	All
Application	Python	Python	3.1.5	All	All	All
Application	Python	Python	3.2.0	All	All	All
Application	Python	Python	3.2.1	All	All	All
Application	Python	Python	3.2.2	All	All	All
Application	Python	Python	3.2.3	All	All	All
Application	Python	Python	3.2.4	All	All	All
Application	Python	Python	3.2.5	All	All	All

Application	Python	Python	3.2.6	All	All	All
Application	Python	Python	3.3.0	All	All	All
Application	Python	Python	3.3.1	All	All	All
Application	Python	Python	3.3.2	All	All	All
Application	Python	Python	3.3.3	All	All	All
Application	Python	Python	3.3.4	All	All	All
Application	Python	Python	3.3.5	All	All	All
Application	Python	Python	3.3.6	All	All	All
Application	Python	Python	3.4.0	All	All	All
Application	Python	Python	3.4.1	All	All	All
Application	Python	Python	3.4.2	All	All	All
Application	Python	Python	3.4.3	All	All	All
Application	Python	Python	3.0	All	All	All
Application	Python	Python	3.0.1	All	All	All
Application	Python	Python	3.1.0	All	All	All
Application	Python	Python	3.1.1	All	All	All
Application	Python	Python	3.1.2	All	All	All
Application	Python	Python	3.1.3	All	All	All
Application	Python	Python	3.1.4	All	All	All
Application	Python	Python	3.1.5	All	All	All
Application	Python	Python	3.2.0	All	All	All
Application	Python	Python	3.2.1	All	All	All
Application	Python	Python	3.2.2	All	All	All
Application	Python	Python	3.2.3	All	All	All
Application	Python	Python	3.2.4	All	All	All
Application	Python	Python	3.2.5	All	All	All
Application	Python	Python	3.2.6	All	All	All
Application	Python	Python	3.3.0	All	All	All
Application	Python	Python	3.3.1	All	All	All
Application	Python	Python	3.3.2	All	All	All
Application	Python	Python	3.3.3	All	All	All
Application	Python	Python	3.3.4	All	All	All
Application	Python	Python	3.3.5	All	All	All
Application	Python	Python	3.3.6	All	All	All
Application	Python	Python	3.4.0	All	All	All

Application	Python	Python	3.4.1	All	All	All
Application	Python	Python	3.4.2	All	All	All
Application	Python	Python	3.4.3	All	All	All
Application	Python	Python	All	All	All	All

cpe:2.3:a:python:python:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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