



CVE-2016-5636

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-5636
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-02 14:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x b

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.451230000 probability, percentile 0.976190000 (date 2026-05-06)

Problem Types: CWE-190 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

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	3.4.4	All	All	All
Application	Python	Python	3.5.0	All	All	All
Application	Python	Python	3.5.1	All	All	All
Application	Python	Python	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
hg.python.org/cpython/raw-file/v2.7.12/Misc/NEWS
Splunk Enterprise 6.4.5 addresses multiple vulnerabilities Splunk
Issue 26171: heap overflow in zipimporter module - Python tracker
Python CVE-2016-5636 Heap Buffer Overflow Vulnerability
Python: Multiple vulnerabilities (GLSA 201701-18) — Gentoo security
Changelog — Python 3.4.5 documentation
[security-announce] openSUSE-SU-2020:0086-1: important: Security update
Red Hat Customer Portal
oss-security - Re: CVE Request: heap overflow in Python zipimport module
Oracle Solaris Bulletin - July 2016
[SECURITY] [DLA 1663-1] python3.4 security update
Changelog — Python 3.5.2 documentation
Apple macOS/OS X Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof URLs, and Obtain Potentially Sensitive Information and I
Splunk Enterprise 6.5.1 addresses multiple OpenSSL vulnerabilities Splunk
oss-security - CVE Request: heap overflow in Python zipimport module

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)