



CVE-2013-7040

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-7040
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-19 14:55:00 UTC
Updated	2019-10-25 11:53:00 UTC
Description	Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to compute hash

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Application	Python	Python	2.7.1	All	All	All
Application	Python	Python	2.7.1	rc1	All	All
Application	Python	Python	2.7.1150	All	All	All
Application	Python	Python	2.7.2	rc1	All	All
Application	Python	Python	2.7.2150	All	All	All
Application	Python	Python	2.7.3	All	All	All
Application	Python	Python	2.7.4	All	All	All
Application	Python	Python	2.7.5	All	All	All
Application	Python	Python	2.7.6	All	All	All
Application	Python	Python	2.7.7	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	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	All	All	All
Application	Python	Python	3.2	alpha	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	3.2.2150	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	3.3	All	All	All
Application	Python	Python	3.3	beta2	All	All
Application	Python	Python	3.3.0	All	All	All
Application	Python	Python	3.3.1	All	All	All
Application	Python	Python	3.3.1	rc1	All	All
Application	Python	Python	3.3.2	All	All	All
Application	Python	Python	3.3.3	All	All	All
Application	Python	Python	3.3.3	rc1	All	All
Application	Python	Python	3.3.3	rc2	All	All
Application	Python	Python	3.3.4	All	All	All
Application	Python	Python	3.3.4	rc1	All	All
Application	Python	Python	3.3.5	-	All	All
Application	Python	Python	3.3.5	rc1	All	All
Application	Python	Python	3.3.5	rc2	All	All
Application	Python	Python	2.7.1	All	All	All
Application	Python	Python	2.7.1	rc1	All	All
Application	Python	Python	2.7.1150	All	All	All
Application	Python	Python	2.7.2	rc1	All	All
Application	Python	Python	2.7.2150	All	All	All
Application	Python	Python	2.7.3	All	All	All
Application	Python	Python	2.7.4	All	All	All
Application	Python	Python	2.7.5	All	All	All
Application	Python	Python	2.7.6	All	All	All
Application	Python	Python	2.7.7	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	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	All	All	All
Application	Python	Python	3.2	alpha	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	3.2.2150	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	3.3	All	All	All
Application	Python	Python	3.3	beta2	All	All
Application	Python	Python	3.3.0	All	All	All
Application	Python	Python	3.3.1	All	All	All
Application	Python	Python	3.3.1	rc1	All	All
Application	Python	Python	3.3.2	All	All	All
Application	Python	Python	3.3.3	All	All	All
Application	Python	Python	3.3.3	rc1	All	All
Application	Python	Python	3.3.3	rc2	All	All
Application	Python	Python	3.3.4	All	All	All
Application	Python	Python	3.3.4	rc1	All	All
Application	Python	Python	3.3.5	-	All	All
Application	Python	Python	3.3.5	rc1	All	All
Application	Python	Python	3.3.5	rc2	All	All

References						
Reference					Source	Link
Python CVE-2013-7040 Information Disclosure Weakness					BID	www.securityfocus.com
oss-security - Re: CPython hash secret can be recovered remotely					MLIST	www.openwall.com

About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support	CONFIRM	support.apple.com
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006	APPLE	lists.apple.com
oss-security - CPython hash secret can be recovered remotely	MLIST	www.openwall.com
Issue 14621: Hash function is not randomized properly - Python tracker	CONFIRM	bugs.python.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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