



CVE-2013-7489

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-7489
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-26 20:15:00 UTC
Updated	2020-07-06 17:50:00 UTC
Description	The Beaker library through 1.11.0 for Python is affected by deserialization of untrusted data, which could lead to arbitrary code execution.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Beakerbrowser	Beaker	All	All	All	All

References

Reference

- oss-security - Python Beaker - Deserialization of Untrusted Data which can lead to Arbitrary code execution
- Insecure data serialization method by default with pickle on Cache · Issue #191 · bbangert/beaker · GitHub
- 1850105 – (CVE-2013-7489) CVE-2013-7489 python-beaker: Deserialization of Untrusted Data which can lead to Arbitrary code execution
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[691143](#) Free Berkeley Software Distribution (FreeBSD) Security Update for py (b54abe9d-7024-4d10-98b2-180cf1717766)

© [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](#).

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