



CVE-2013-4346

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

Summary

CVE	CVE-2013-4346
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-20 14:55:00 UTC
Updated	2023-02-13 00:28:00 UTC
Description	The Server.verify_request function in SimpleGeo python-oauth2 does not check the nonce, which allows remote attackers to

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Urbanairship	Python-oauth2	-	All	All	All
Application	Urbanairship	Python-oauth2	-	All	All	All

References

Reference	Source
Red Hat Customer Portal	MISC
1007746 – (CVE-2013-4346) CVE-2013-4346 python-oauth2: _check_signature() ignores the nonce value when validating signed urls	MISC
Red Hat Customer Portal	MISC
python-oauth2 Signed URL Nonce Verification Security Bypass Vulnerability	BID
Duplicate nonce check on Server.verify_request() · Issue #129 · joestump/python-oauth2 · GitHub	MISC
CVE-2013-4346 - Red Hat Customer Portal	MISC
oss-security - Re: cve requests for python-oauth2	MLIS
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

997508 Python (Pip) Security Update for oauth2 (GHSA-4433-4cxq-vv73)

© [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](#)