



# CVE-2016-1494

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

## Summary

<b>CVE</b>	CVE-2016-1494
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-01-13 15:59:00 UTC
<b>Updated</b>	2019-05-31 17:27:00 UTC
<b>Description</b>	The verify function in the RSA package for Python (Python-RSA) before 3.3 allows attackers to spoof signatures with a sma

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Application	<a href="#">Python</a>	<a href="#">Rsa</a>	All	All	All	All
Application	<a href="#">Python</a>	<a href="#">Rsa</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE Request: python-rsa signature forgery	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third Party Advi
Python-RSA CVE-2016-1494 Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB E

[SECURITY] Fedora 22 Update: python-rsa-3.3-2.fc22	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third Party Advisory
Bleichenbacher'06 signature forgery in python-rsa	MISC	<a href="https://blog.filippo.io">blog.filippo.io</a>	Exploit, Third Party Advisory
404 — Bitbucket	CONFIRM	<a href="https://bitbucket.org">bitbucket.org</a>	Patch, Third Party Advisory
openSUSE-SU-2016:0108-1: moderate: Security update for python-rsa	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party Advisory
[SECURITY] Fedora 23 Update: python-rsa-3.3-2.fc23	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third Party Advisory
oss-security - Re: CVE Request: python-rsa signature forgery	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing List, Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)