CVE-2016-1494

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-1494
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-13 15:59:00 UTC
Updated	2019-05-31 17:27:00 UTC
Description	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	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Python	Rsa	All	All	All	All
Application	Python	Rsa	All	All	All	All

References

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

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

No vendor comments have been submitted for this CVE.

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