CVE-2013-2037

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-2037
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-18 21:55:00 UTC
Updated	2018-12-06 20:53:00 UTC
Description	httplib2 0.7.2, 0.8, and earlier, after an initial connection is made, does not verify that the server hostname matches a doma

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Application	Httplib2 Project	Httplib2	0.8	All	All	All
Application	Httplib2 Project	Httplib2	All	All	All	All
Application	Httplib2 Project	Httplib2	0.8	All	All	All

References

Reference
Issue 282 - httplib2 - SSL certificate hostname mismatch is checked only once - A comprehensive HTTP client library in Python - Google Proje
USN-1948-1: httplib2 vulnerability | Ubuntu
python-httplib2 CVE-2013-2037 SSL Certificate Validation Security Bypass Vulnerability

Bug #1175272 “requests permitted after invalid certificate is re...” : Bugs : httplib2
#706602 - python-httplib2: CVE-2013-2037 - Debian Bug report logs
oss-sec: Re: CVE Request: httplib2 ssl cert incorrect error handling
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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