CVE-2021-21240

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

Summary

CVE	CVE-2021-21240
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-08 20:15:00 UTC
Updated	2021-02-12 14:56:00 UTC
Description	httplib2 is a comprehensive HTTP client library for Python. In httplib2 before version 0.19.0, a malicious server which respo

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Httplib2 Project	Httplib2	All	All	All	All
Application	Httplib2 Project	Httplib2	All	All	All	All

References

Reference	Source	Link
parse auth headers using pyparsing instead of regexp · httplib2/httplib2@bd9ee25 · GitHub	MISC	github.com
Regular Expression Denial of Service (REDoS) in httplib2 · Advisory · httplib2/httplib2 · GitHub	CONFIRM	github.com
parse auth headers using pyparsing instead of regexp by temoto · Pull Request #182 · httplib2/httplib2 · GitHub	MISC	github.com
httplib2 · PyPI	MISC	pypi.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183347 Debian Security Update for python-httplib2 (CVE-2021-21240)

501902 Alpine Linux Security Update for py3-httplib2

750016 SUSE Enterprise Linux Security Update for python-httplib2 (SUSE-SU-2021:1637-1)

750086 SUSE Enterprise Linux Security Update for python-httplib2 (SUSE-SU-2021:1806-1)

750087 SUSE Enterprise Linux Security Update for python-httplib2 (SUSE-SU-2021:1807-1)

750195 OpenSUSE Security Update for python-httplib2 (openSUSE-SU-2021:0772-1)

750764 OpenSUSE Security Update for python-httplib2 (openSUSE-SU-2021:1806-1)

982955 Python (pip) Security Update for httplib2 (GHSA-93xj-8mrv-444m)