



CVE-2020-7655

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

Summary

CVE	CVE-2020-7655
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-21 15:15:00 UTC
Updated	2020-05-21 20:21:00 UTC
Description	netius prior to 1.17.58 is vulnerable to HTTP Request Smuggling. HTTP pipelining issues and request smuggling attacks m

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hive	Netius	All	All	All	All
Application	Hive	Netius	All	All	All	All

References

Reference	Source	Link	Tags
HTTP Request Smuggling in netius Snyk	MISC	snyk.io	Patch, Third Party Advisory
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.

Legacy QID Mappings

982206 Python (pip) Security Update for netius (GHSA-wm2m-xrrp-j74c)

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