Tinyproxy HTTP request parsing desynchronization via case-sensitive Transfer-Encoding handling

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

Summary

CVE	CVE-2026-31842
State	PUBLISHED
Assigner	TuranSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 12:16:21 UTC
Updated	2026-04-07 13:20:11 UTC
Description	Tinyproxy through 1.11.3 is vulnerable to HTTP request parsing desynchronization due to a case-sensitive comparison of th

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from 309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000460000 probability, percentile 0.142610000 (date 2026-04-07)

Problem Types: CWE-444 | CWE-444 CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Version	Source	Type	Score	Severity	Vector
4.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H
3.1	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	Secondary	7.8		AV:N/AC:L/Au:N/C:N/I:N/A:C
2.0	CNA	CVSS	7.8		AV:N/AC:L/Au:N/C:N/I:N/A:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tinyproxy Project	Tinyproxy	affected 1.11.3 custom	all

References

Reference	Source	Link	Tags
github.com/tinyproxy/tinyproxy	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	github.com	
datatracker.ietf.org/doc/html/rfc7230	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	datatracker.ietf.org	
github.com/tinyproxy/tinyproxy/issues/604	309f9ea4-e3e9-4c6c-b79d-e8eb01244f2c	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Muxammadiyev G'iyosiddin (en)

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

© 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 registred 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**